



Nationally Critical Infrastructure needs Secure Hardware

aka Democracy is a Critical System

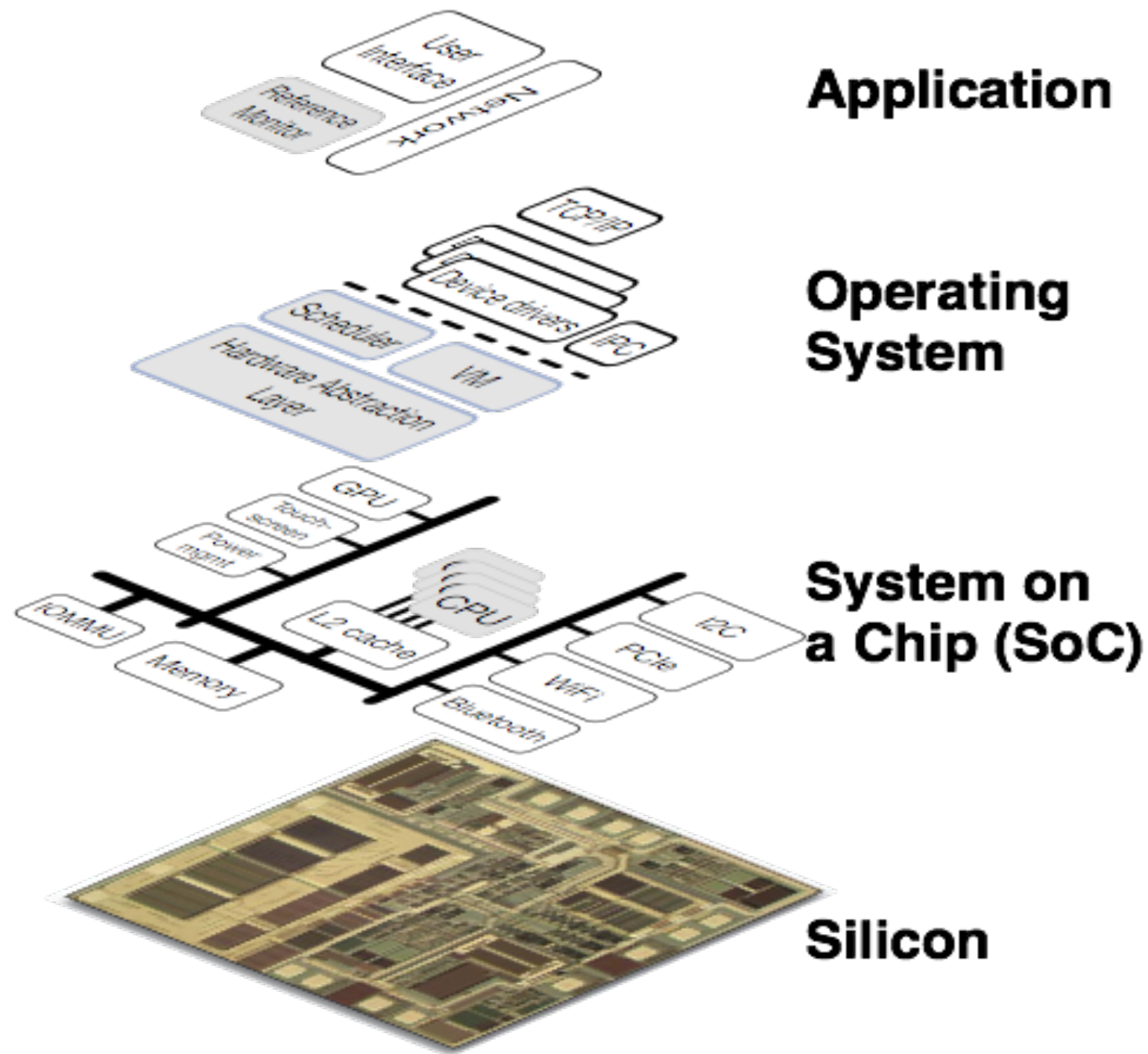
Joe Kiniry

Galois and Free & Fair

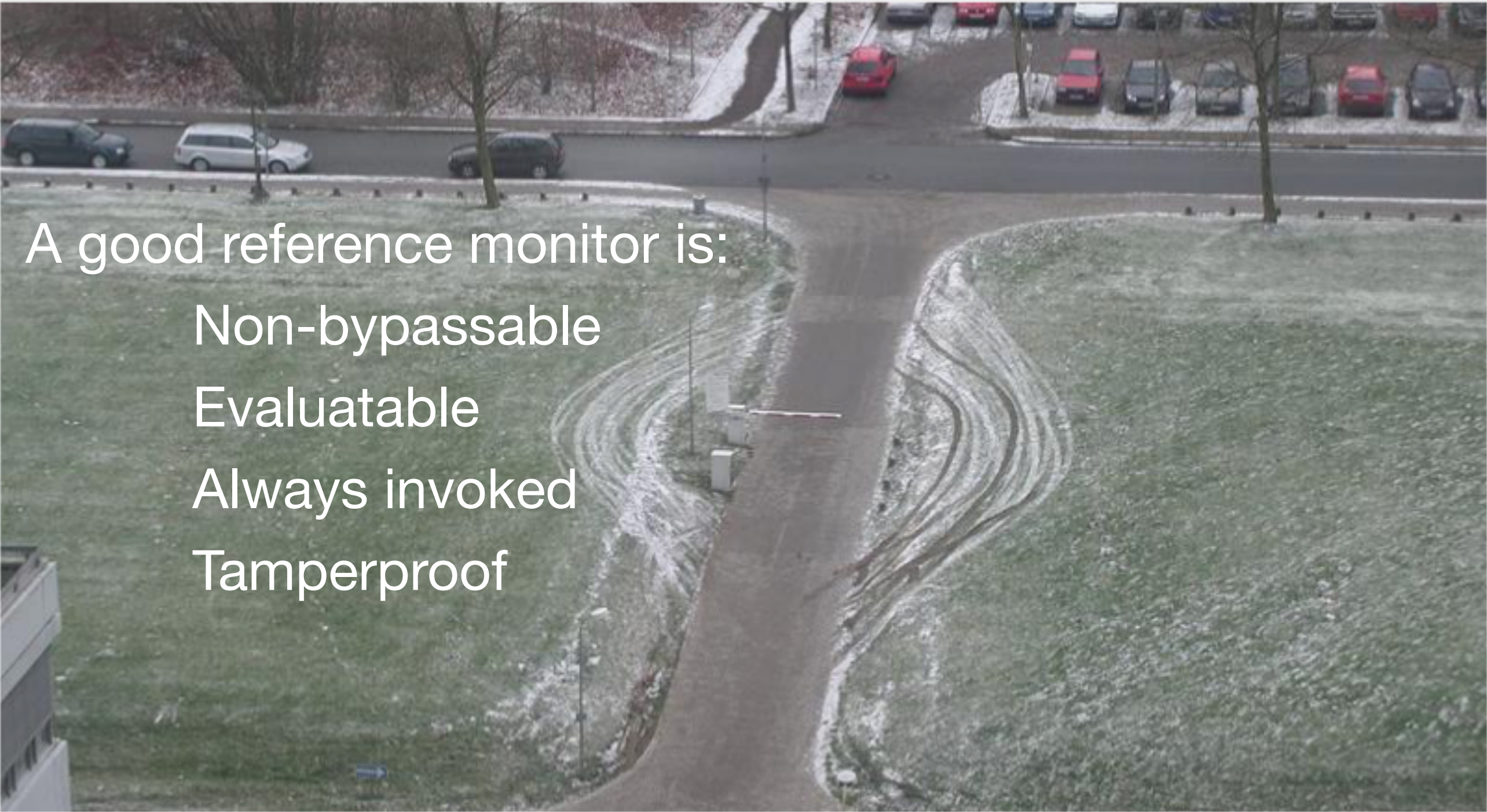
Cybersecurity of Nationally Critical Infrastructure: Assurance Cases Built on Sand

Cybersecurity of Nationally Critical Infrastructure: Assurance Castles Built on Sand

Where is the Security?



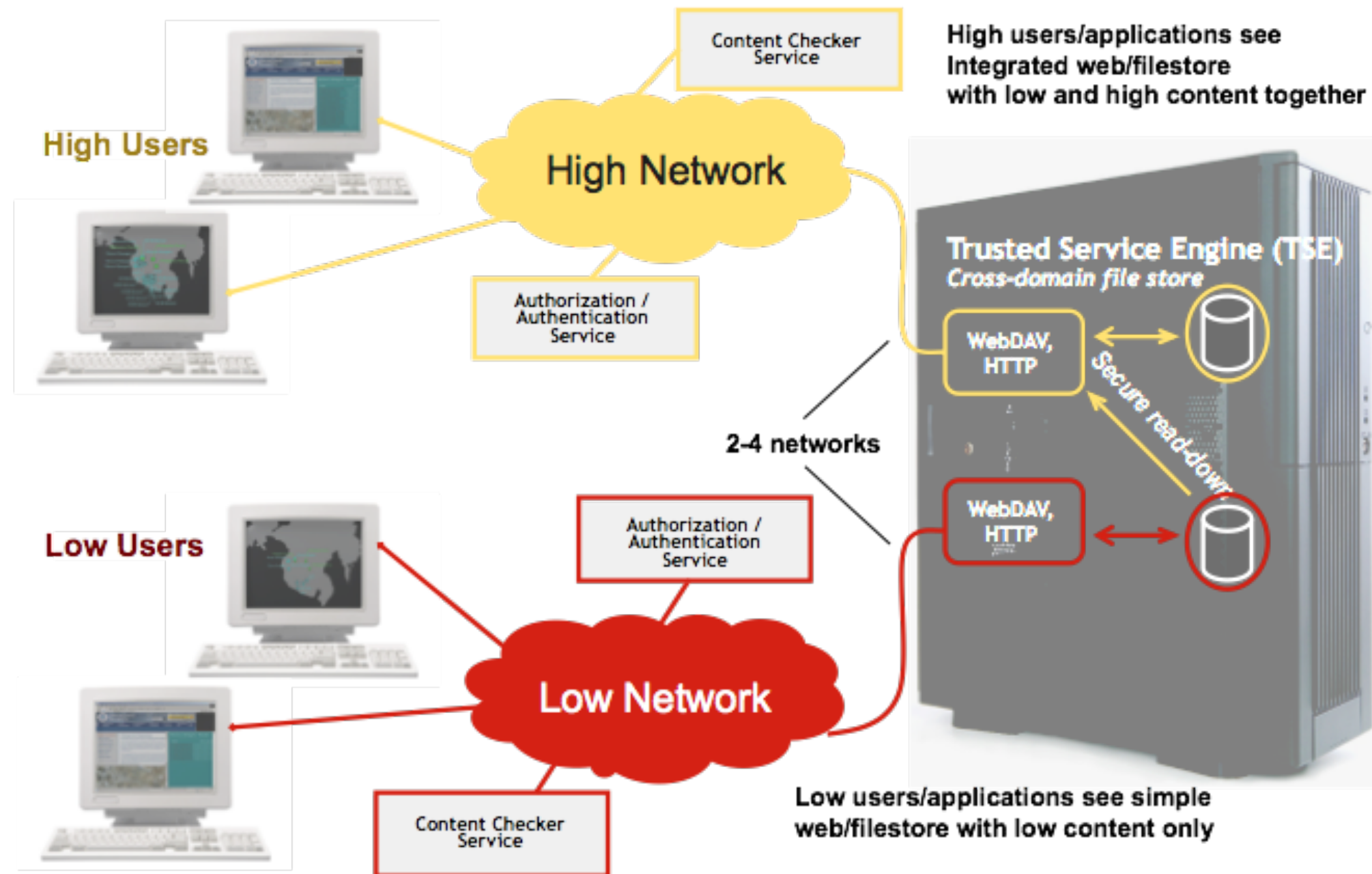
Market Opportunity: Bad Reference Monitors

An aerial photograph of a road intersection. A road with a reference monitor barrier (a small white box with a red and white striped arm) crosses a grassy area. The road is paved and has some snow or ice on it. In the background, there is a parking lot with several cars and a road with more cars. The grassy area is green with some snow or ice patches.

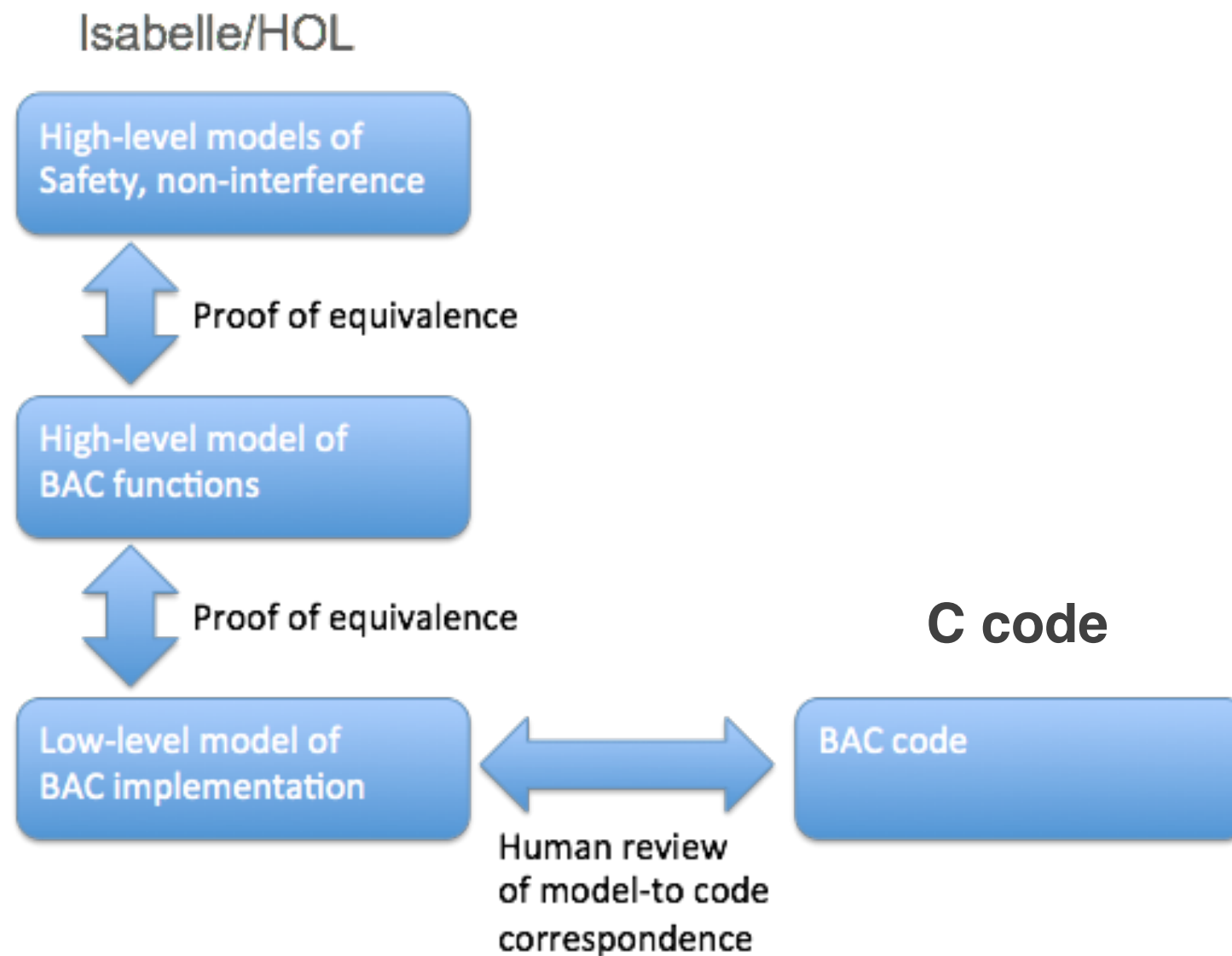
A good reference monitor is:

- Non-bypassable
- Evaluatable
- Always invoked
- Tamperproof

Galois' Trusted Services Engine

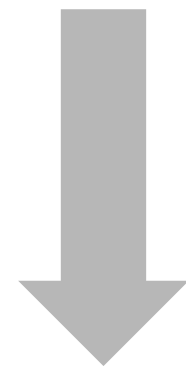


Block Access Controller Assurance Architecture

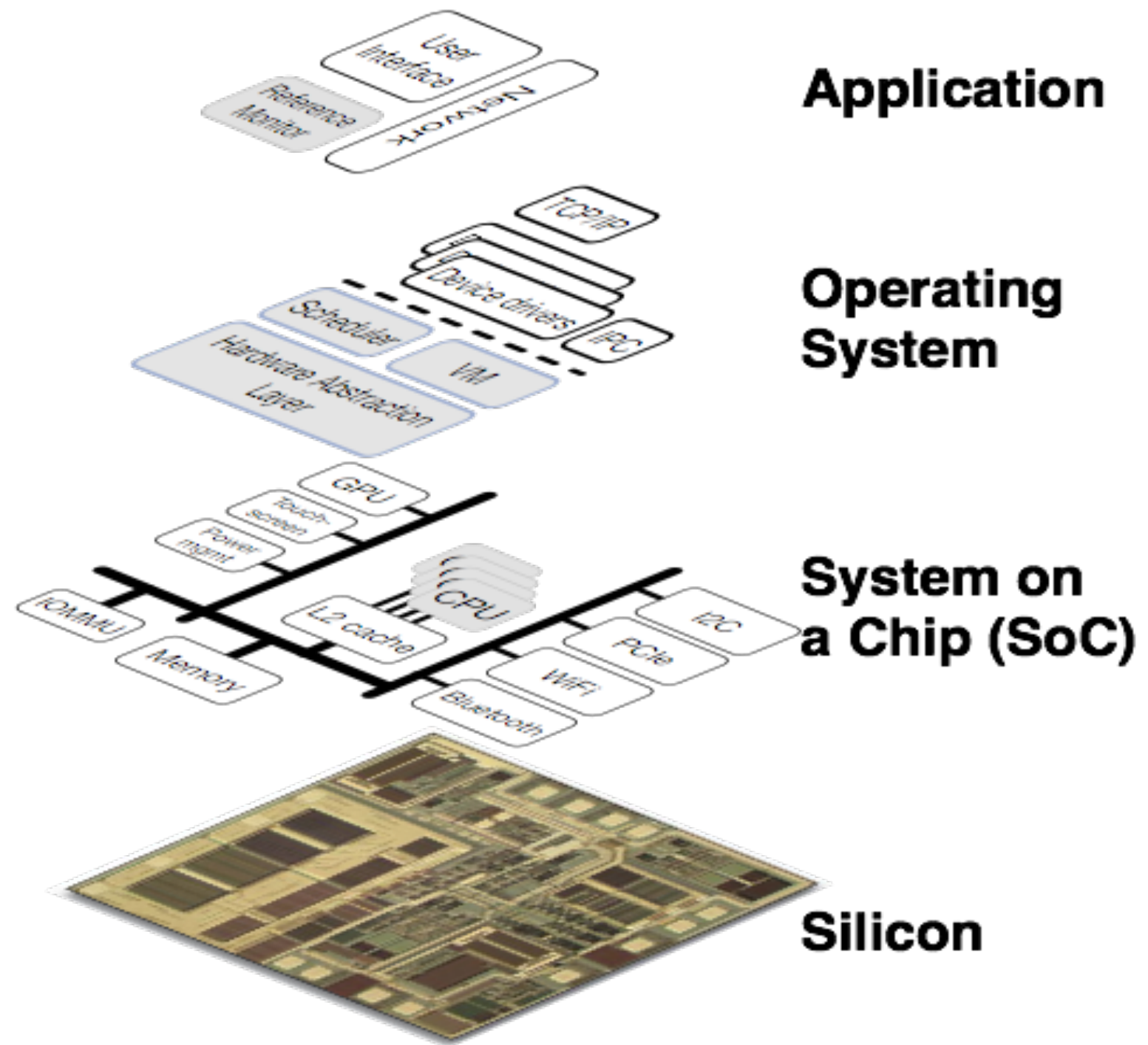


- testing is weak evidence about the actual system
 - residual worry: have I tested enough?
- proofs are strong evidence about a model of the system
 - residual worry: is my model accurate?

Where is the Security?



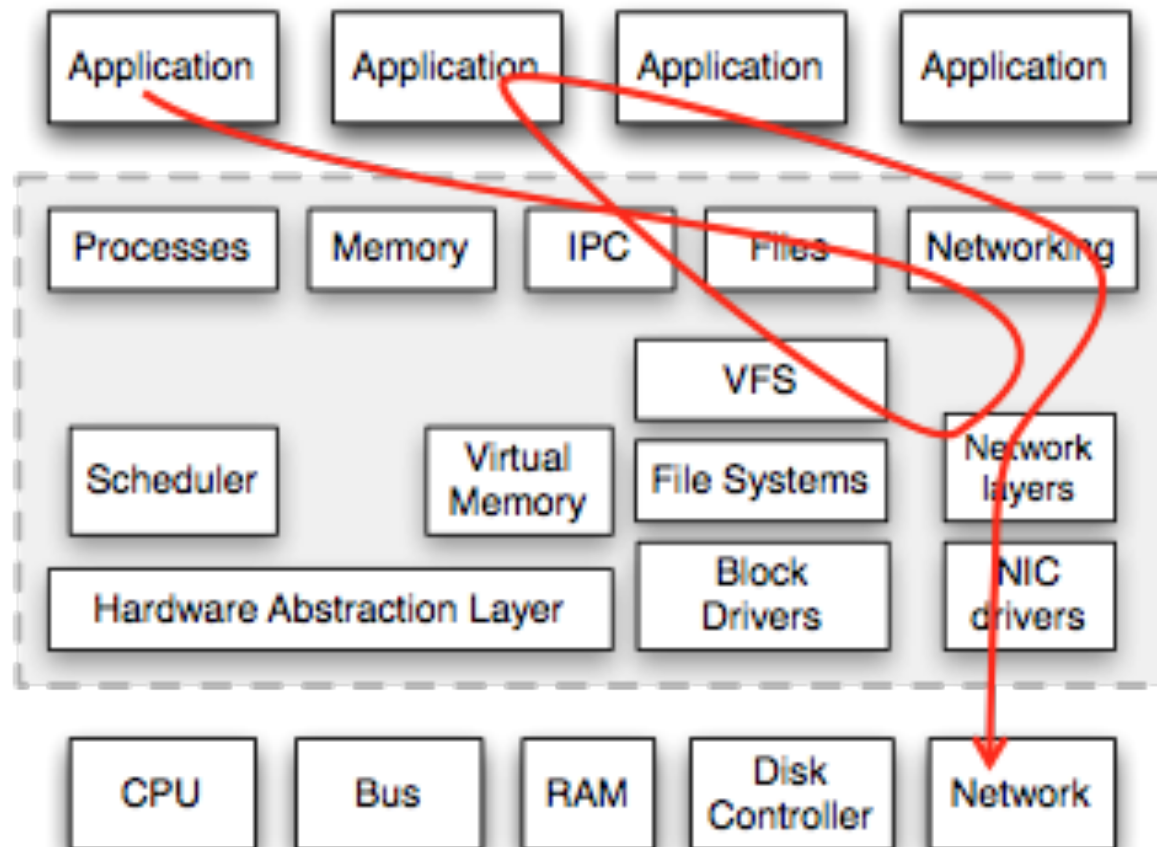
*What kind of
OS
can we trust?*



MILS: High-assurance Policy Enforcement

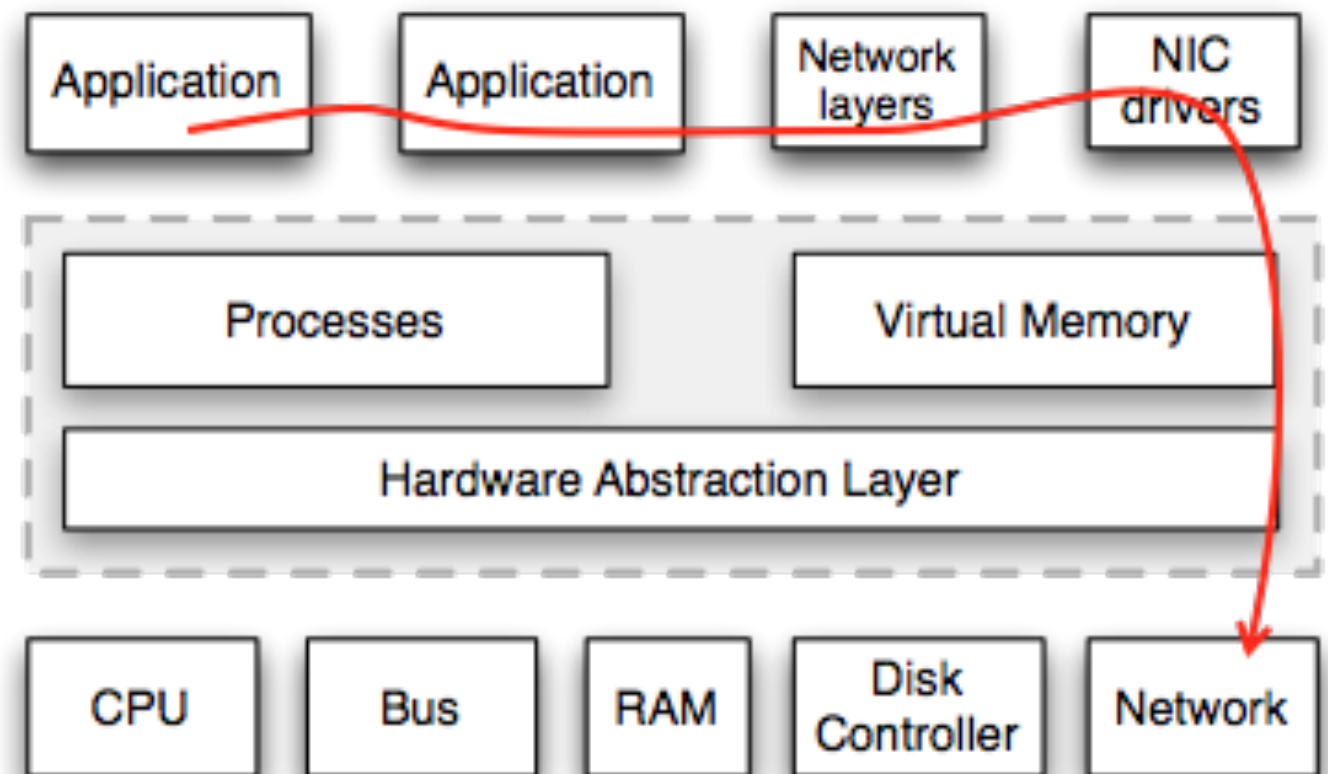
Monolithic OS approach

Secure domain

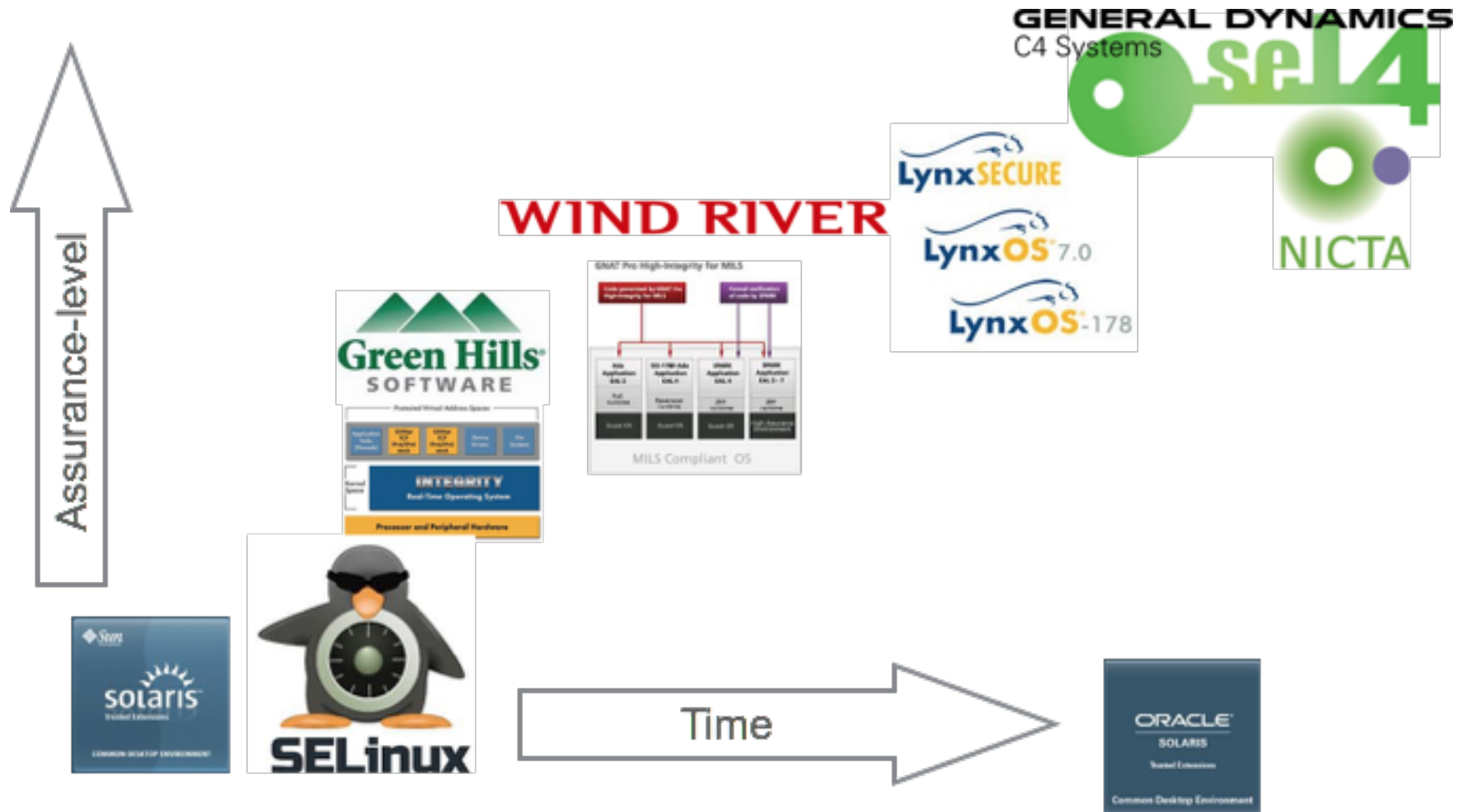


MILS approach

Secure domain



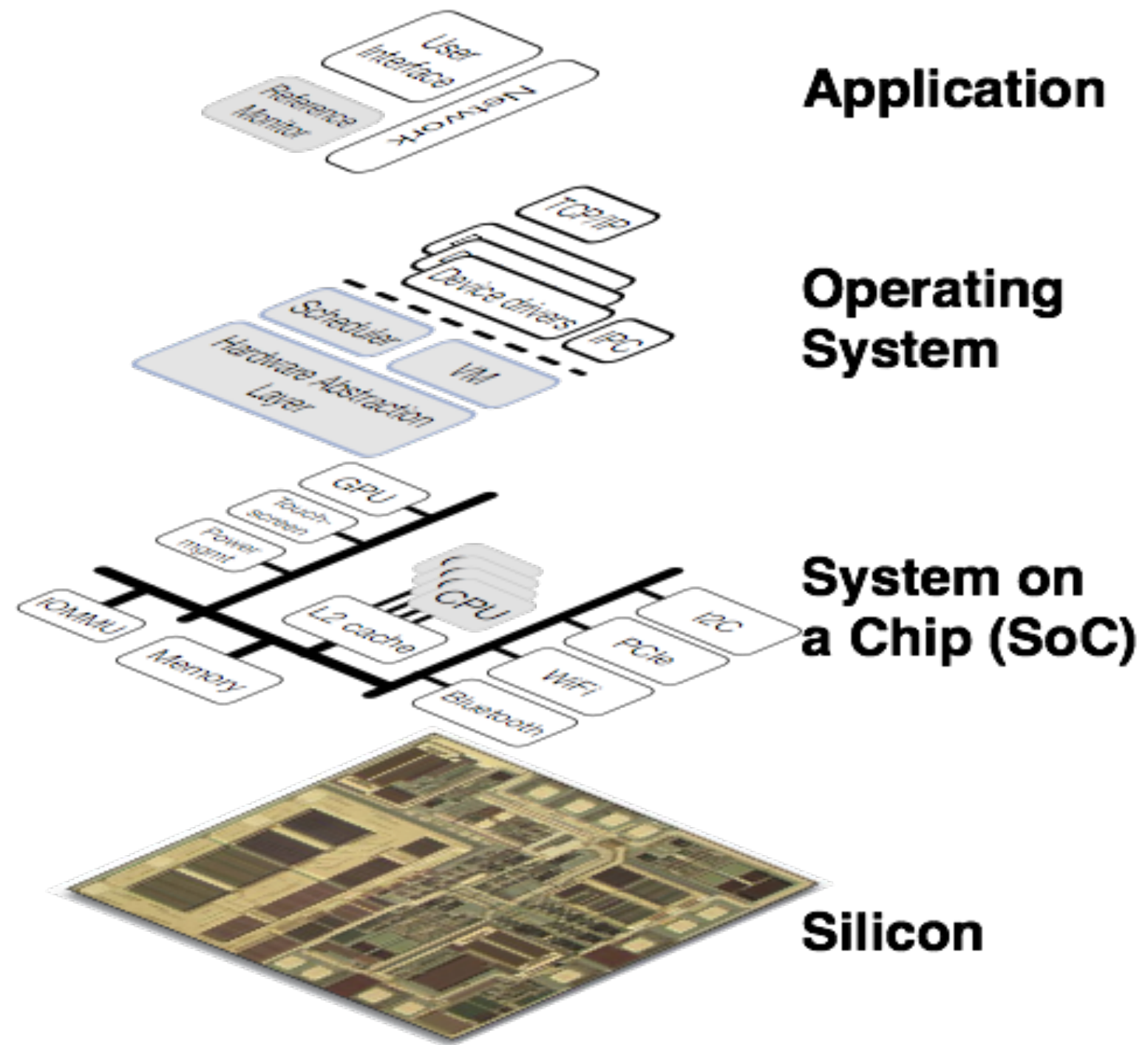
Operating System Options



Where is the Security?



What kind of hardware can we trust?



System Assurance

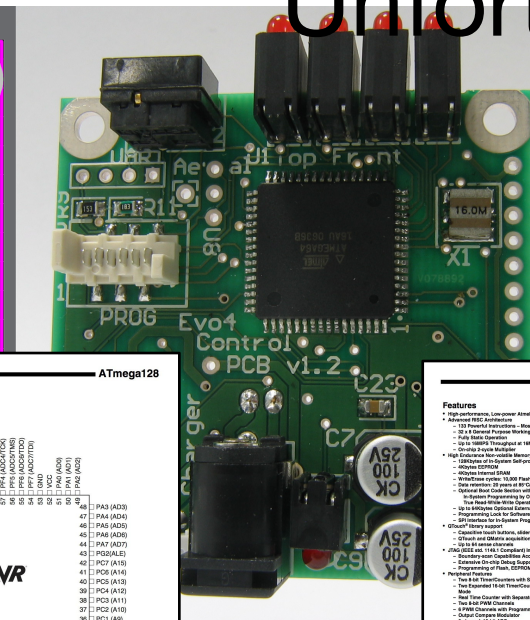
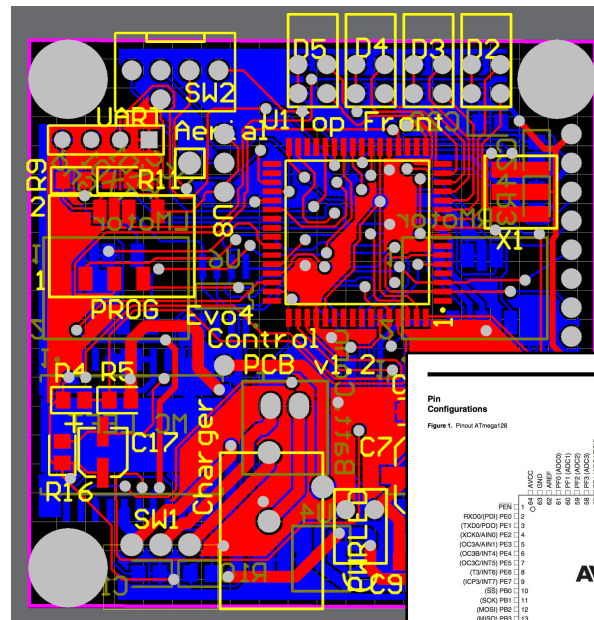
system assurance is about
the assurance of your
hardware & firmware & software

Unfortunately...



Linux

not see my
WARRANT



ATmega128

Pin Configurations

Figure 1. Pinout ATmega128

PIN	FUNCTION	PIN	FUNCTION
1	AVCC	46	PA4 (A03)
2	AREF	47	PA5 (A04)
3	ADSC	48	PA6 (A05)
4	ADIF	49	PA7 (A06)
5	ADIF	50	PA8 (A07)
6	ADIF	51	PA9 (A08)
7	ADIF	52	PA10 (A09)
8	ADIF	53	PA11 (A10)
9	ADIF	54	PA12 (A11)
10	ADIF	55	PA13 (A12)
11	ADIF	56	PA14 (A13)
12	ADIF	57	PA15 (A14)
13	ADIF	58	PA16 (A15)
14	ADIF	59	PA17 (A16)
15	ADIF	60	PA18 (A17)
16	ADIF	61	PA19 (A18)
17	ADIF	62	PA20 (A19)
18	ADIF	63	PA21 (A20)
19	ADIF	64	PA22 (A21)
20	ADIF	65	PA23 (A22)
21	ADIF	66	PA24 (A23)
22	ADIF	67	PA25 (A24)
23	ADIF	68	PA26 (A25)
24	ADIF	69	PA27 (A26)
25	ADIF	70	PA28 (A27)
26	ADIF	71	PA29 (A28)
27	ADIF	72	PA30 (A29)
28	ADIF	73	PA31 (A30)
29	ADIF	74	PA32 (A31)
30	ADIF	75	PA33 (A32)
31	ADIF	76	PA34 (A33)
32	ADIF	77	PA35 (A34)
33	ADIF	78	PA36 (A35)
34	ADIF	79	PA37 (A36)
35	ADIF	80	PA38 (A37)
36	ADIF	81	PA39 (A38)
37	ADIF	82	PA40 (A39)
38	ADIF	83	PA41 (A40)
39	ADIF	84	PA42 (A41)
40	ADIF	85	PA43 (A42)
41	ADIF	86	PA44 (A43)
42	ADIF	87	PA45 (A44)
43	ADIF	88	PA46 (A45)
44	ADIF	89	PA47 (A46)
45	ADIF	90	PA48 (A47)
46	ADIF	91	PA49 (A48)
47	ADIF	92	PA50 (A49)
48	ADIF	93	PA51 (A50)
49	ADIF	94	PA52 (A51)
50	ADIF	95	PA53 (A52)
51	ADIF	96	PA54 (A53)
52	ADIF	97	PA55 (A54)
53	ADIF	98	PA56 (A55)
54	ADIF	99	PA57 (A56)
55	ADIF	100	PA58 (A57)
56	ADIF	101	PA59 (A58)
57	ADIF	102	PA60 (A59)
58	ADIF	103	PA61 (A60)
59	ADIF	104	PA62 (A61)
60	ADIF	105	PA63 (A62)
61	ADIF	106	PA64 (A63)
62	ADIF	107	PA65 (A64)
63	ADIF	108	PA66 (A65)
64	ADIF	109	PA67 (A66)
65	ADIF	110	PA68 (A67)
66	ADIF	111	PA69 (A68)
67	ADIF	112	PA70 (A69)
68	ADIF	113	PA71 (A70)
69	ADIF	114	PA72 (A71)
70	ADIF	115	PA73 (A72)
71	ADIF	116	PA74 (A73)
72	ADIF	117	PA75 (A74)
73	ADIF	118	PA76 (A75)
74	ADIF	119	PA77 (A76)
75	ADIF	120	PA78 (A77)
76	ADIF	121	PA79 (A78)
77	ADIF	122	PA80 (A79)
78	ADIF	123	PA81 (A80)
79	ADIF	124	PA82 (A81)
80	ADIF	125	PA83 (A82)
81	ADIF	126	PA84 (A83)
82	ADIF	127	PA85 (A84)
83	ADIF	128	PA86 (A85)
84	ADIF	129	PA87 (A86)
85	ADIF	130	PA88 (A87)
86	ADIF	131	PA89 (A88)
87	ADIF	132	PA90 (A89)
88	ADIF	133	PA91 (A90)
89	ADIF	134	PA92 (A91)
90	ADIF	135	PA93 (A92)
91	ADIF	136	PA94 (A93)
92	ADIF	137	PA95 (A94)
93	ADIF	138	PA96 (A95)
94	ADIF	139	PA97 (A96)
95	ADIF	140	PA98 (A97)
96	ADIF	141	PA99 (A98)
97	ADIF	142	PA100 (A99)
98	ADIF	143	PA101 (A100)
99	ADIF	144	PA102 (A101)
100	ADIF	145	PA103 (A102)
101	ADIF	146	PA104 (A103)
102	ADIF	147	PA105 (A104)
103	ADIF	148	PA106 (A105)
104	ADIF	149	PA107 (A106)
105	ADIF	150	PA108 (A107)
106	ADIF	151	PA109 (A108)
107	ADIF	152	PA110 (A109)
108	ADIF	153	PA111 (A110)
109	ADIF	154	PA112 (A111)
110	ADIF	155	PA113 (A112)
111	ADIF	156	PA114 (A113)
112	ADIF	157	PA115 (A114)
113	ADIF	158	PA116 (A115)
114	ADIF	159	PA117 (A116)
115	ADIF	160	PA118 (A117)
116	ADIF	161	PA119 (A118)
117	ADIF	162	PA120 (A119)
118	ADIF	163	PA121 (A120)
119	ADIF	164	PA122 (A121)
120	ADIF	165	PA123 (A122)
121	ADIF	166	PA124 (A123)
122	ADIF	167	PA125 (A124)
123	ADIF	168	PA126 (A125)
124	ADIF	169	PA127 (A126)
125	ADIF	170	PA128 (A127)
126	ADIF	171	PA129 (A128)
127	ADIF	172	PA130 (A129)
128	ADIF	173	PA131 (A130)
129	ADIF	174	PA132 (A131)
130	ADIF	175	PA133 (A132)
131	ADIF	176	PA134 (A133)
132	ADIF	177	PA135 (A134)
133	ADIF	178	PA136 (A135)
134	ADIF	179	PA137 (A136)
135	ADIF	180	PA138 (A137)
136	ADIF	181	PA139 (A138)
137	ADIF	182	PA140 (A139)
138	ADIF	183	PA141 (A140)
139	ADIF	184	PA142 (A141)
140	ADIF	185	PA143 (A142)
141	ADIF	186	PA144 (A143)
142	ADIF	187	PA145 (A144)
143	ADIF	188	PA146 (A145)
144	ADIF	189	PA147 (A146)
145	ADIF	190	PA148 (A147)
146	ADIF	191	PA149 (A148)
147	ADIF	192	PA150 (A149)
148	ADIF	193	PA151 (A150)
149	ADIF	194	PA152 (A151)
150	ADIF	195	PA153 (A152)
151	ADIF	196	PA154 (A153)
152	ADIF	197	PA155 (A154)
153	ADIF	198	PA156 (A155)
154	ADIF	199	PA157 (A156)
155	ADIF	200	PA158 (A157)
156	ADIF	201	PA159 (A158)
157	ADIF	202	PA160 (A159)
158	ADIF	203	PA161 (A160)
159	ADIF	204	PA162 (A161)
160	ADIF	205	PA163 (A162)
161	ADIF	206	PA164 (A163)
162	ADIF	207	PA165 (A164)
163	ADIF	208	PA166 (A165)
164	ADIF	209	PA167 (A166)
165	ADIF	210	PA168 (A167)
166	ADIF	211	PA169 (A168)
167	ADIF	212	PA170 (A169)
168	ADIF	213	PA171 (A170)
169	ADIF	214	PA172 (A171)
170	ADIF	215	PA173 (A172)
171	ADIF	216	PA174 (A173)
172	ADIF	217	PA175 (A174)
173	ADIF	218	PA176 (A175)
174	ADIF	219	PA177 (A176)
175	ADIF	220	PA178 (A177)
176	ADIF	221	PA179 (A178)
177	ADIF	222	PA180 (A179)
178	ADIF	223	PA181 (A180)
179	ADIF	224	PA182 (A181)
180	ADIF	225	PA183 (A182)
181	ADIF	226	PA184 (A183)
182	ADIF	227	PA185 (A184)
183	ADIF	228	PA186 (A185)
184	ADIF	229	PA187 (A186)
185	ADIF	230	PA188 (A187)
186	ADIF	231	PA189 (A188)
187	ADIF	232	PA190 (A189)
188	ADIF	233	PA191 (A190)
189	ADIF	234	PA192 (A191)
190	ADIF	235	PA193 (A192)
191	ADIF	236	PA194 (A193)
192	ADIF	237	PA195 (A194)
193	ADIF	238	PA196 (A195)
194	ADIF	239	PA197 (A196)
195	ADIF	240	PA198 (A197)
196	ADIF	241	PA199 (A198)
197	ADIF	242	PA200 (A199)
198	ADIF	243	PA201 (A200)
199	ADIF	244	PA202 (A201)
200	ADIF	245	PA203 (A202)
201	ADIF	246	PA204 (A203)
202	ADIF	247	PA205 (A204)
203	ADIF	248	PA206 (A205)
204	ADIF	249	PA207 (A206)
205	ADIF	250	PA208 (A207)
206	ADIF	251	PA209 (A208)
207	ADIF	252	PA210 (A209)
208	ADIF	253	PA211 (A210)
209	ADIF	254	PA212 (A211)
210	ADIF	255	PA213 (A212)
211	ADIF	256	PA214 (A213)
212	ADIF	257	PA215 (A214)
213	ADIF	258	PA216 (A215)
214	ADIF	259	PA217 (A216)
215	ADIF	260	PA218 (A217)
216	ADIF	261	PA219 (A218)
217	ADIF	262	PA220 (A219)
218	ADIF	263	PA221 (A220)
219	ADIF	264	PA222 (A221)
220	ADIF	265	PA223 (A222)
221	ADIF	266	PA224 (A223)
222	ADIF	267	PA225 (A224)
223	ADIF	268	PA226 (A225)
224	ADIF	269	PA227 (A226)
225	ADIF	270	PA228 (A227)
226	ADIF	271	PA229 (A228)
227	ADIF	272	PA230 (A229)
228	ADIF	273	PA231 (A230)
229	ADIF	274	PA232 (A231)
230	ADIF	275	PA233 (A232)
231	ADIF	276	PA234 (A233)
232	ADIF	277	PA235 (A234)
233	ADIF	278	PA236 (A235)
234	ADIF	279	PA237 (A236)
235	ADIF	280	PA238 (A237)
236	ADIF	281	PA239 (A238)
237	ADIF	282	PA240 (A239)
238	ADIF	283	PA241 (A240)
239	ADIF	284	PA242 (A241)
240	ADIF	285	PA243 (A242)
241	ADIF	286	PA244 (A243)
242	ADIF	287	PA245 (A244)
243	ADIF	288	PA246 (A245)
244	ADIF	289	PA247 (A246)
245	ADIF	290	PA248 (A247)
246	ADIF	291	PA249 (A248)
247	ADIF	292	PA250 (A249)
248	ADIF	293	PA251 (A250)
249	ADIF	294	PA252 (A251)
250	ADIF	295	PA253 (A252)
251	ADIF	296	PA254 (A253)
252	ADIF	297	PA255 (A254)
253	ADIF	298	PA256 (A255)
254	ADIF	299	PA257 (A256)
255	ADIF	300	PA258 (A257)
256	ADIF	301	PA259 (A258)
257	ADIF	302	PA260 (A259)
258	ADIF	303	PA261 (A260)
259	ADIF	304	PA262 (A261)
260	ADIF	305	PA263 (A262)
261	ADIF	306	PA264 (A263)
262	ADIF	307	PA265 (A264)
263	ADIF	308	PA266 (A265)
264	ADIF	309	PA267 (A266)
265	ADIF	310	PA268 (A267)
266	ADIF	311	PA269 (A268)
267	ADIF	312	PA270 (A269)
268	ADIF	313	PA271 (A270)
269	ADIF	314	PA272 (A271)
270	ADIF	315	PA273 (A272)
271	ADIF	316	PA274 (A273)
272	ADIF	317	PA275 (A274)
273	ADIF	318	PA276 (A275)
274	ADIF	319	PA277 (A276)
275	ADIF	320	PA278 (A277)
276	ADIF	321	PA279 (A278)
277	ADIF	322	PA280 (A279)
278	ADIF	323	PA281 (A280)
279	ADIF	324	PA282 (A281)
280	ADIF	325	PA283 (A282)
281	ADIF	326	PA284 (A283)
282	ADIF	327	PA285 (A284)
283	ADIF	328	PA286 (A285)
284	ADIF	329	PA287 (A286)
285	ADIF	330	PA288 (A287)
286	ADIF	331	PA289 (A288)
287	ADIF	332	PA290 (A289)
288	ADIF	333	PA291 (A290)
289	ADIF	334	PA292 (A291)
290	ADIF	335	PA293 (A292)
291	ADIF</		

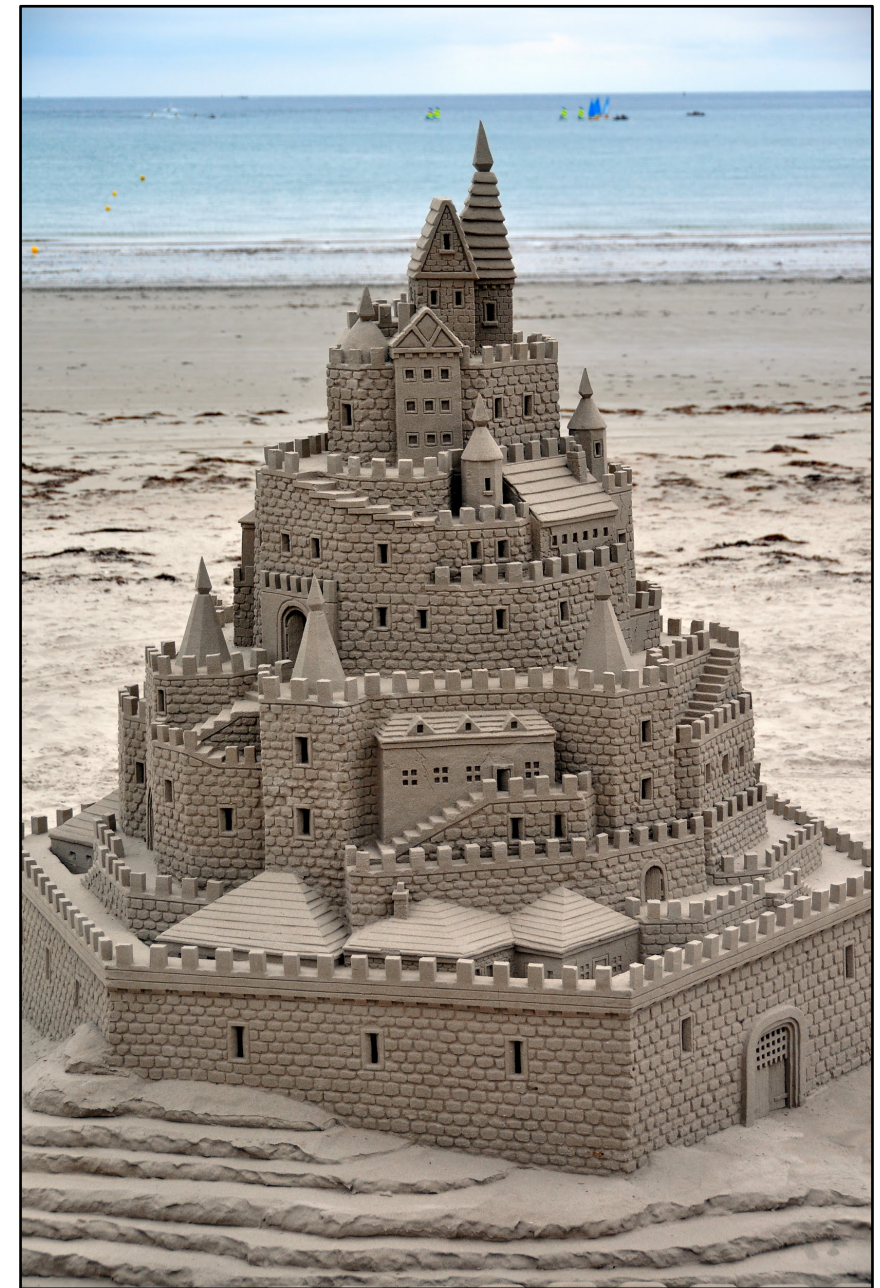
System Assurance

- system assurance is about the assurance of your hardware & software
 - today we have faith-based assurance cases



Assurance Cases Built on Sand

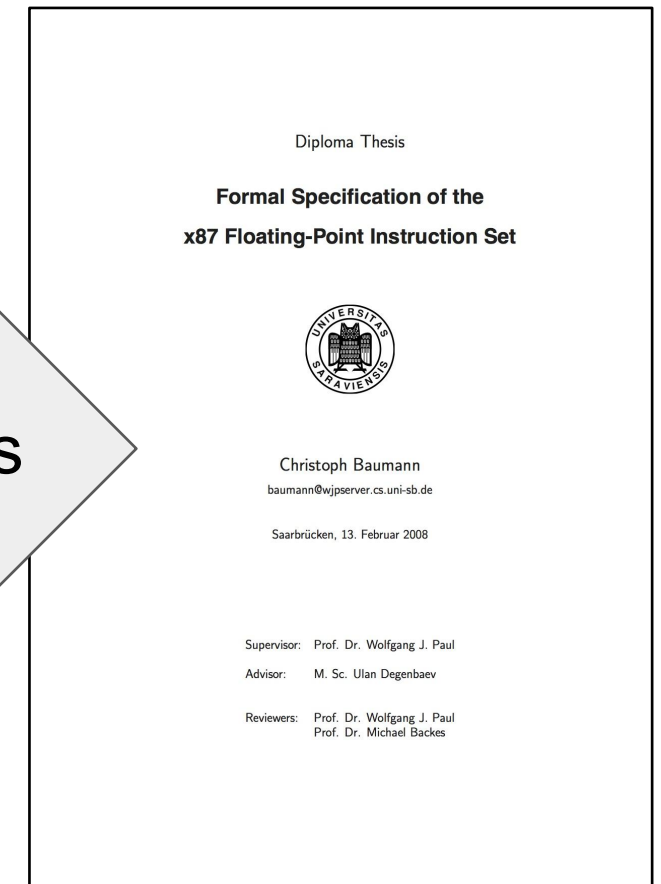
- assurance cases depend upon evidence
- hardware assurance means: tested, simulated, some formal verification of equivalence, fabled it somewhere I cannot trust, and it looks like it works
- software formal verification means formal proof that an implementation does exactly as specified — no more, no less (plus testing, simulation, etc.)
- software assurance rely upon firmware and hardware's guarantees
- firmware is opaque and has no guarantees, and hardware does not come with a reliable specification
- vendors rarely wish to share specifications
- consequently...
our assurance cases are build on sand



The Bridge Between Our Worlds is Broken



dozens of person years



A Solution Proposed This Decade

- provide the high level formal models from your verification process
- refine EDA tools to produce evidence

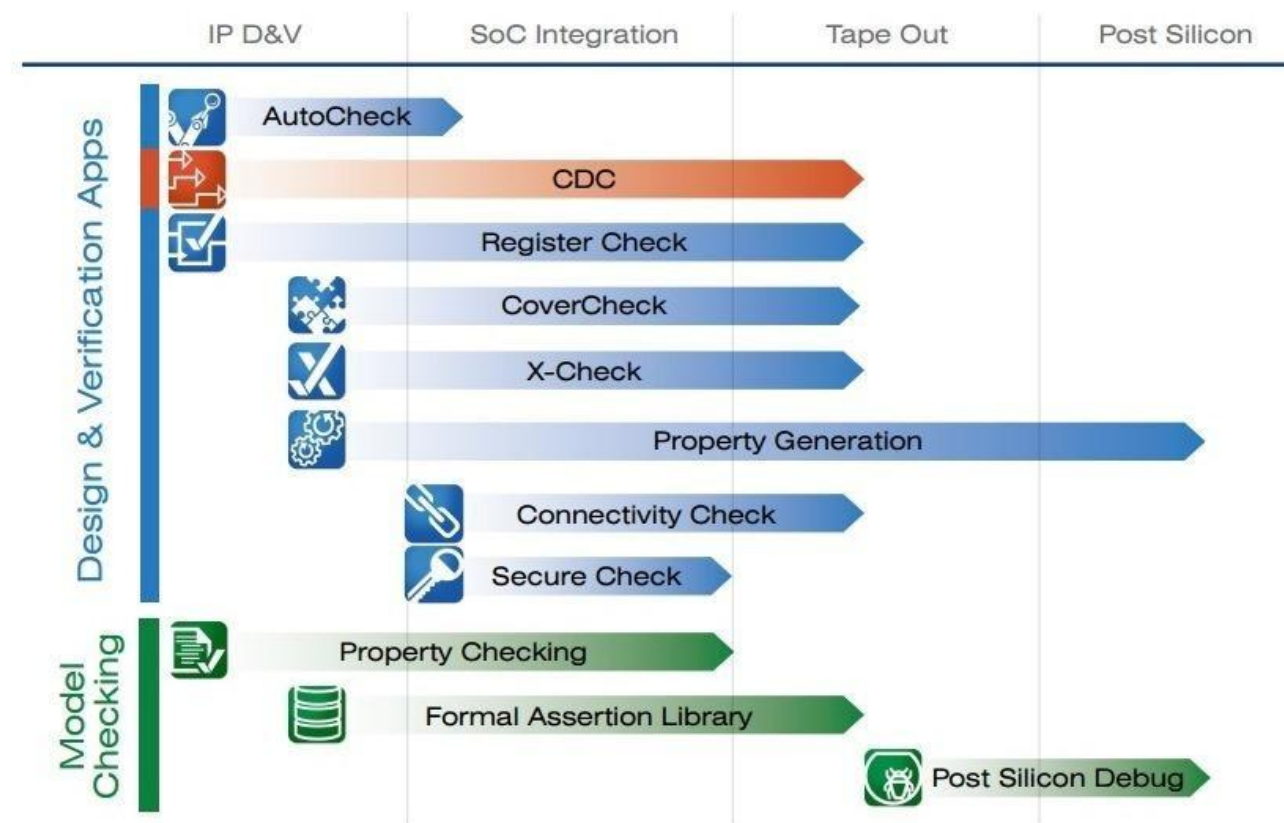


A Solution Proposed This Decade

- provide the high level formal models from your verification process
- refine EDA tools to produce evidence

IA-32
Formal
Model

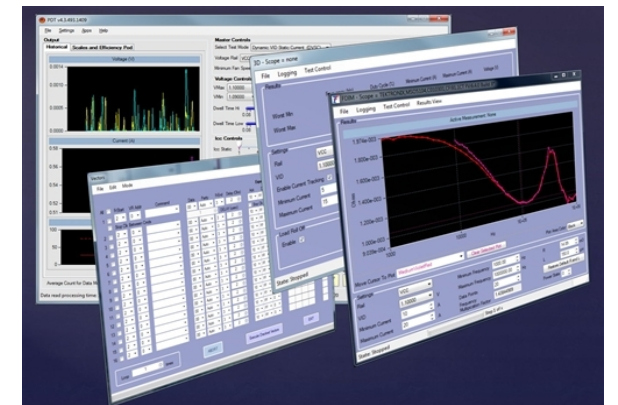
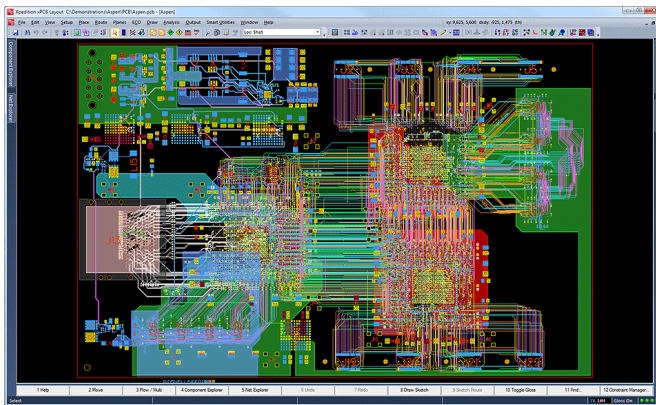
la-32.hol
la-32.sv
la-32.hs



+ evidence that checked properties are valid

Implications on Assurance and Capabilities

- decrease resource waste due to duplication of enormous effort and increase quality
- more intelligent and cost-effective co-design process, methods, and tools
- end-to-end assurance cases open up new markets and products, both government and consumer



New Versions! With Proofs!
We Guarantee It!

A 2014 Call to Action

- let's build assurance cases on a firm foundation
- improve communication between assurance and software formal verification experts and hardware designers and verification engineers
- integrate formal verification tools and techniques into hardware verification
- demonstrate exemplar formal assurance cases for non-trivial systems

DARPA SSITH: System Security Integrated Through Hardware

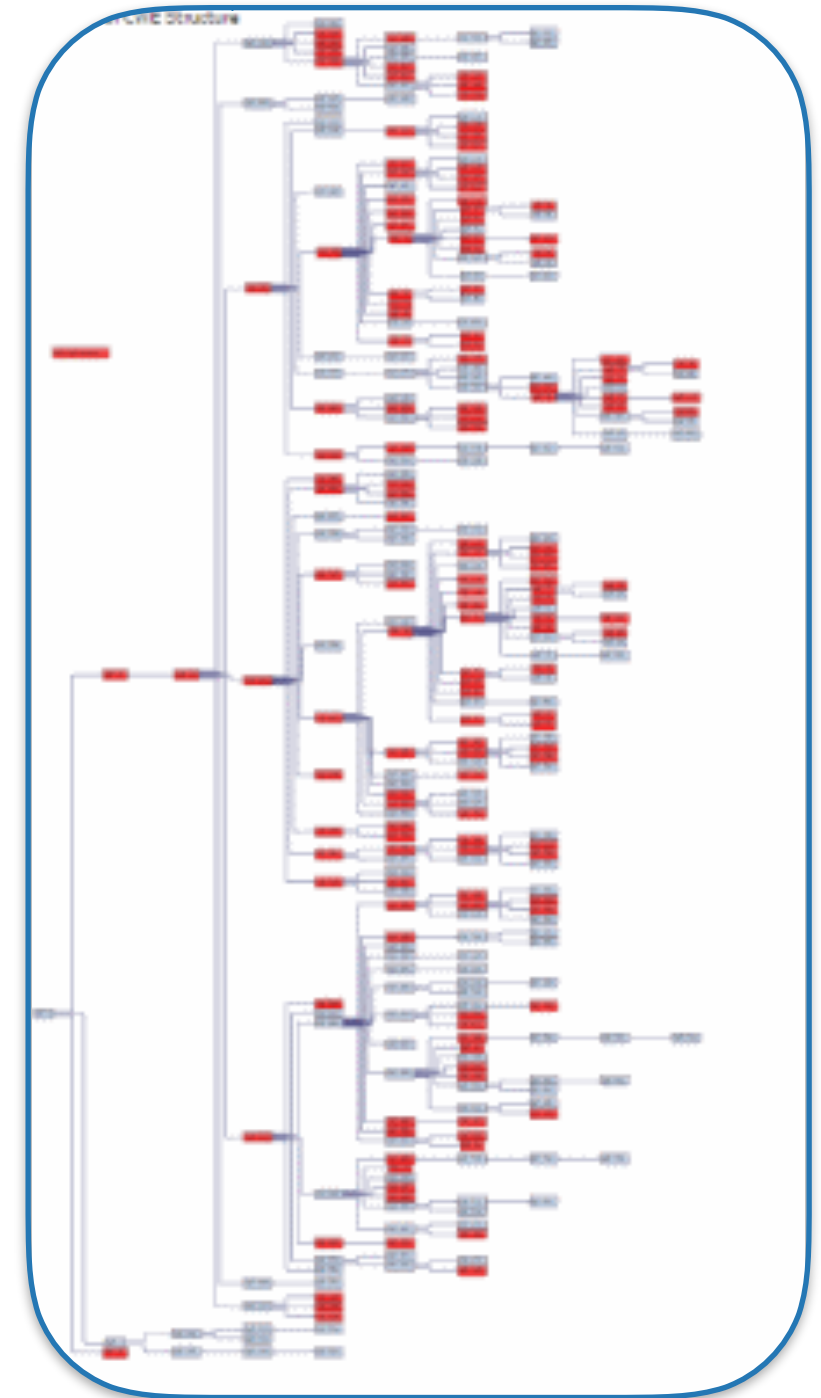
SSITH in a Nutshell

- secure hardware FTW!
- goal is to eliminate most classes of software vulnerabilities
- open source, soft-core RISC-V on FPGAs as the demo platform
- six teams developing 18 SoCs
- each team augments three baseline RISC-V SoCs to make them secure
- a 32 bit microcontroller and two 64 bit CPUs (one OOO)
- security approaches are all over the map, including tagging, enclaves, novel crypto, and AI



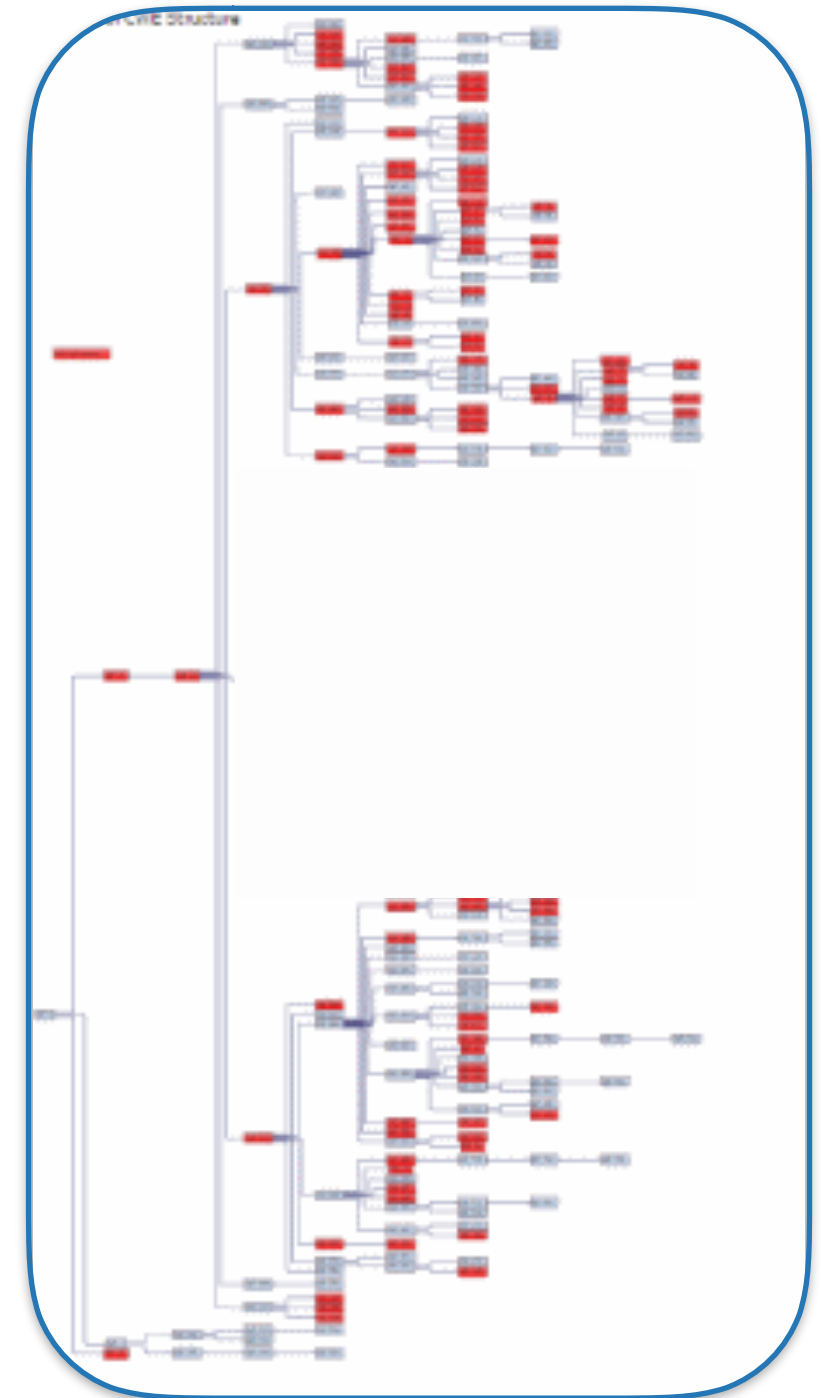
Mitigating Software Vulnerabilities with Hardware

- SSITH CPUs must be backwards compatible & run existing binaries
- these binaries have vast numbers of exploitable vulnerabilities
- software vulnerabilities are classified using NIST CWE classes via NIST, which form a subtyping tree depicted at right



Mitigating Software Vulnerabilities with Hardware

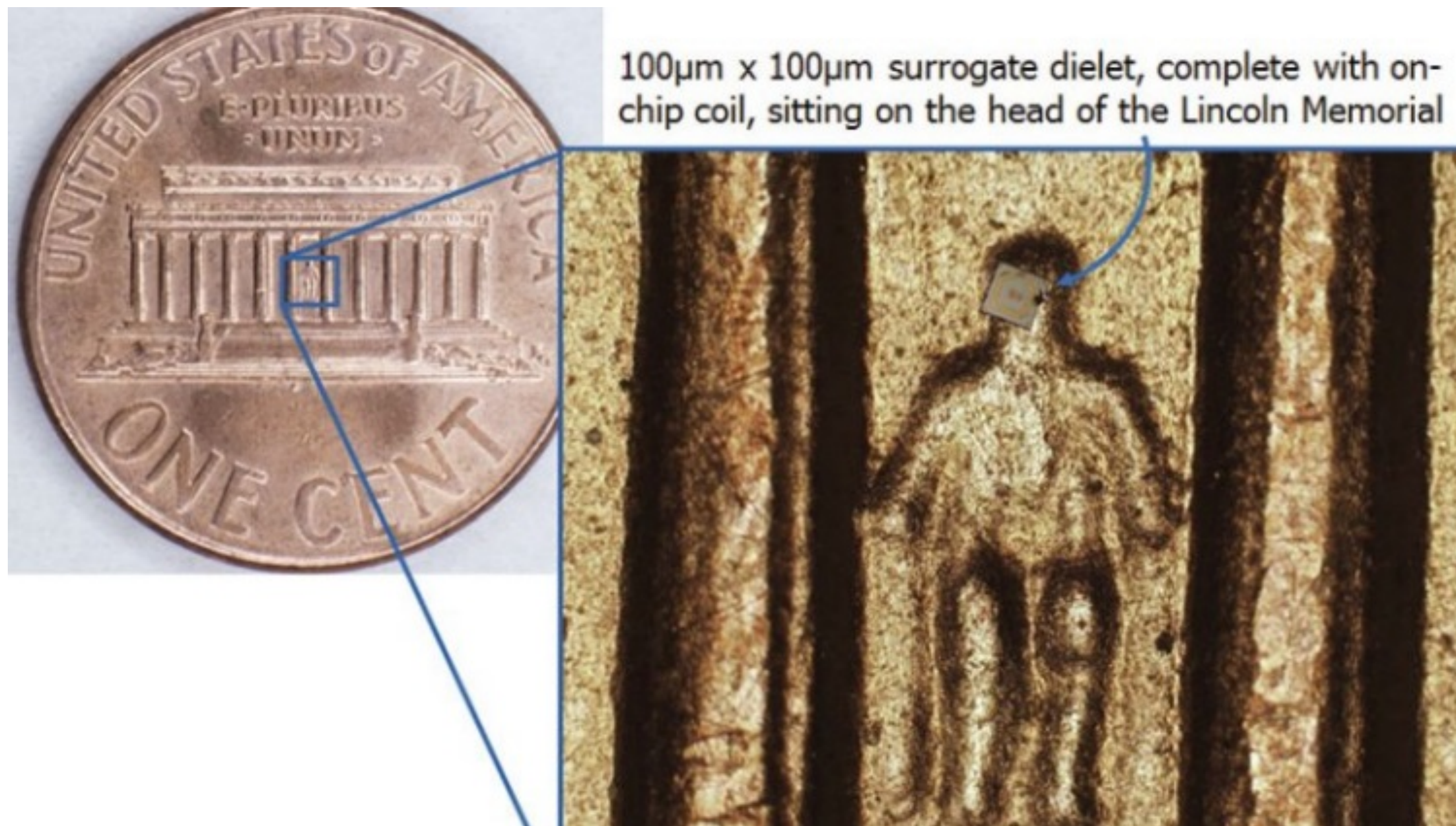
- SSITH CPUs must be backwards compatible & run existing binaries
- these binaries have vast numbers of exploitable vulnerabilities
- software vulnerabilities are classified using NIST CWE classes via NIST, which form a subtyping tree depicted at right
- SSITH CPUs mitigate specific CWE types, thus pruning subtrees of software vulnerabilities away



Security-Related R&D

- several mechanized formal specifications of the ISA and (possibly secure) cores
 - MIT, SRI, Cambridge, Galois, Symbiotic EDA
- several cryptographic extension implementations
 - from ad hoc to formally synthesized, from not tested at all to formally verified, from leaky to side channel-free
- secure boot implementations and enclaves
 - from ports of large historic nightmares to formally verified implementations
- SSITH teams are creating dozens of different secure SoCs that include dozens of security features
- other programs are working on circuit obfuscation, tamper detection, and mitigation of supply channel attacks

DARPA SHIELD



RISC-V: An Open Platform for Security R&D

What is RISC-V?

- RISC-V (pronounced *risk-five*) is the fifth major RISC design effort at UC Berkeley
- high-quality, license-free, royalty-free RISC ISA
- used to design everything from tiny microcontrollers to multicore servers with domain specific accelerators
- development started in Summer 2010
- early workshops were a couple of handfuls of graduate students and faculty from Berkeley & MIT
- the latest RISC-V Summit had >1,000 attendees and hundreds of companies were represented
- **a platform for doing open secure hardware R&D and product development for very low cost**

Why is RISC-V Interesting?

- **simple**
 - far smaller than other commercial ISAs
- **clean-slate design**
 - clear separation between user and privileged ISA
 - avoids μ architecture or technology-dependent features
- **modular**
 - small standard base ISA
 - multiple standard extensions
- **designed for extensibility/specialization**
 - variable-length instruction encoding
 - vast opcode space available for instruction-set extensions
- **stable**
 - base and standard extensions are frozen
 - additions via optional extensions, not new versions

RISC-V + Security

- top-level Security Standing Committee to provide leadership, guidance, and strategy
 - Chair: Helena Handschuh (Rambus)
Vice Chair: Joe Kiniry (Galois)
- two active Task Groups
 - cryptographic extensions
 - Chair: Richard Newell (Microchip/Microsemi)
Vice Chair: Dan Zimmerman (Galois)
 - broad set of crypto algorithms via instructions
 - leverages work from vector extension
 - trusted execution environment
 - Chair: Joe Xie (NVIDIA)
 - different shaped enclaves for different kinds of SoCs (microcontroller — server-class CPUs)

Democracy is a Critical System

The State of Voting System Security

- USA
 - handful of vendors: ES&S, Hart-Intercivic, Dominion Voting, Unisyn, Clear Ballot Group
- International
 - two main vendors: Scytl and Smartmatic
- the average voting system is either...
 - COTS running on unpatched Windows or Linux
 - custom hardware designed and manufactured in 1990s using microcontrollers & unpatched RTOS

Evoting System Flavors

- bespoke low-tech voting systems
 - NL's Nedap, India's EVM
- optical mark-sense voting systems
 - electronic ballot markers & digital pens
- DRM (with or without paper audit trails)
- remote/internet voting systems
- end-to-end, voter-verifiable systems
 - Punchscan, Scantegrity, Prêt à Voter, ElectionGuard

Bespoke Systems



- computers used in elections since the mid-1980s
- voting machines are simple computers
- 8 bit CPUs, minimal RAM and store, custom PCBs, no operating system

Lever Machines



Optical Scanners

**State of Connecticut
Official Ballot**



Fairfield, Connecticut

Municipal Election

November 8, 2011

Voting District 1

Sheet 1 of 1

OFFICE →	1 First Selectman
PARTY ↓	
DEMOCRATIC	<input type="radio"/> 1A Michael C. Tetreau
REPUBLICAN	<input type="radio"/> 1B Rob Bellitto
INDEPENDENT	<input type="radio"/> 1C Hugh F. Dolan
GREEN	1D
WORKING FAMILIES	1E
WRITE-IN VOTES →	<input type="radio"/> 1F



13 Town Plan and Zoning Commission Four Year Term Vote for Any Two	14 Town Plan and Zoning Commission Two Year Term	15 Town Plan and Zoning Commission Two Year Term
<input type="radio"/> 13A Patricia M. Jacobson	<input type="radio"/> 14A Sally E. Parker	<input type="radio"/> 15A Anita Rappoport
<input type="radio"/> 13B Matthew Wagner	<input type="radio"/> 14B Bryan LeClerc	<input type="radio"/> 15B Douglas Soutar
13C	14C	15C
13D	14D	15D
13E	14E	15E
<input type="radio"/> 13F	<input type="radio"/> 14F	<input type="radio"/> 15F

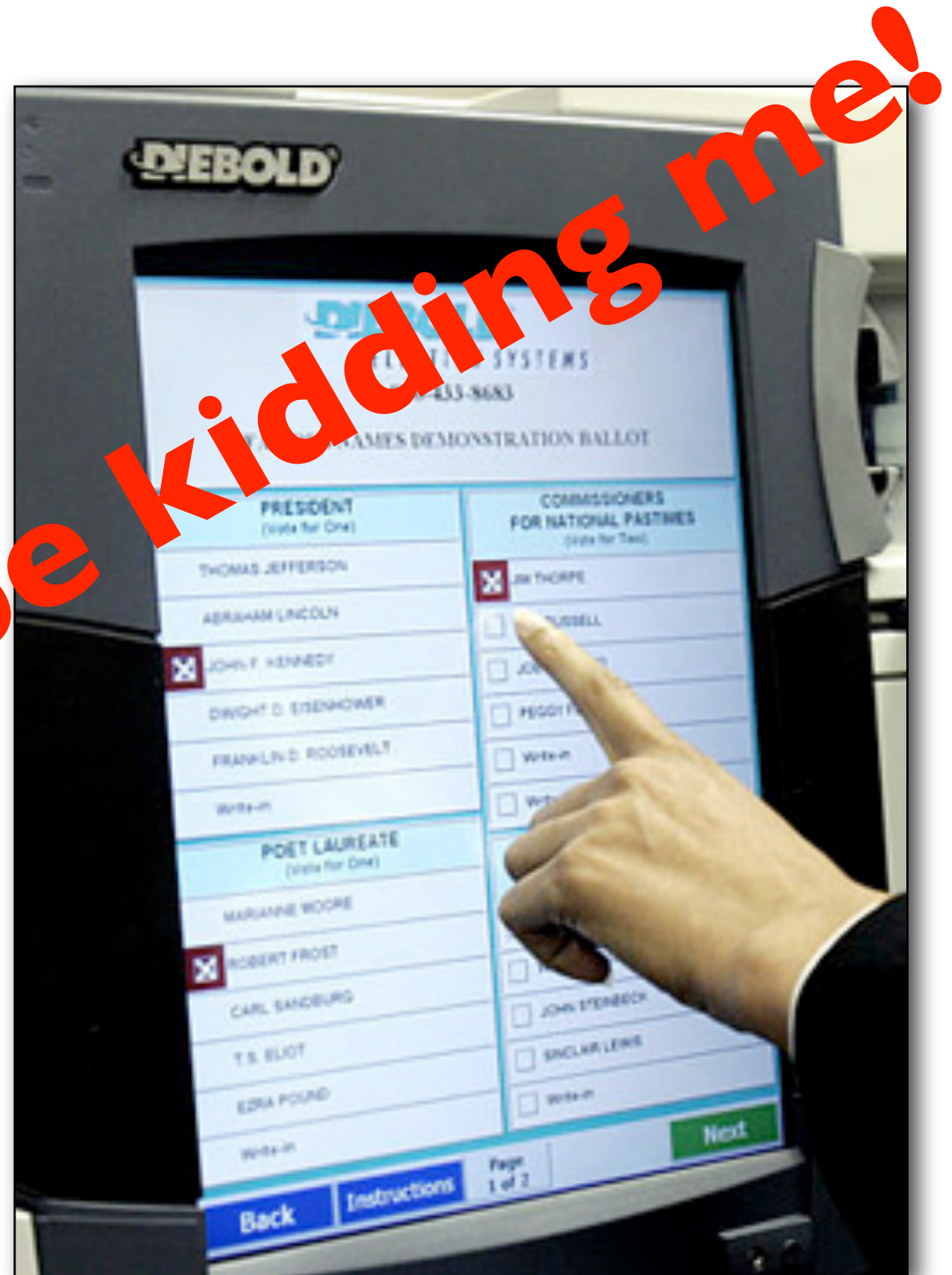
Be sure to complete your vote on the reverse side of this ballot.

DREs and VVPAT



Typical DRM Machine

- terribly built
- runs Windows
- uses commodity hardware
- no paper ballots
- voter must trust that it works correctly

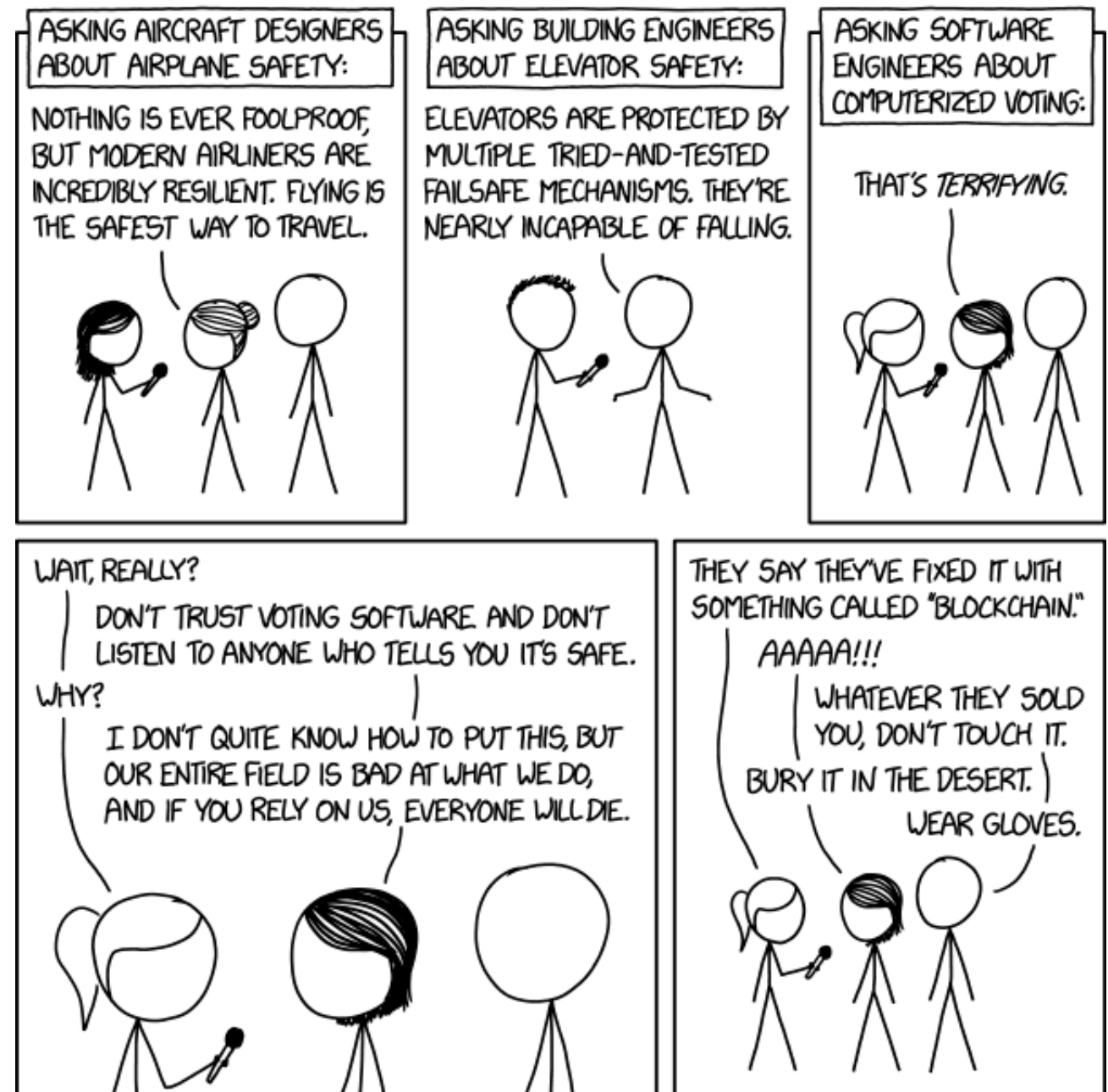


State-of-the-Art Assessment

- personally assessed many evolving software systems (commercial and research) and read reports on hardware systems
- these systems, in the general, have
- poor software engineering practices
- no rigorous validation and verification
- little traceability to requirements
- questionable certification
- poor quality and security

But Wait!

- Internet Voting!
 - Estonia
 - Australia
 - Switzerland
- Blockchain!
 - Smartmatic
 - Voatz
 - Votem
 - FollowMyVote
 - ...and other tripe...



Estonia Sample Code

```
def analyze(ik, vote, votebox):  
  
    # TODO: implement security checks  
    # such as verifying the correct size  
    # of the encrypted vote  
  
    return []
```


DEF CON Voting Village



DEF CON Voting Village




DEF CON Voting Village

THE WALL STREET JOURNAL.

U.S. Edition | June 13, 2019 | Print Edition | Video

Subscribe | Sign In

Home World **U.S.** Politics Economy Business Tech Markets Opinion Life & Arts Real Estate WSJ. Magazine

Search 

U.S.

Voting Machine Used in Half of U.S. Is Vulnerable to Attack, Report Finds

The flaw in Election Systems & Software's Model 650 high-speed ballot-counting machine was detailed in 2007



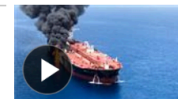
The Election Systems & Software Model 650 Central Scanner & Tabulator has a flaw that could make it vulnerable to a cyberattack, according to a new report. PHOTO: ROBERT MCMILLAN/THE WALL STREET JOURNAL

By [Robert McMillan](#) and [Dustin Volz](#)

Updated Sept. 27, 2018 8:40 a.m. ET

Most Popular Videos

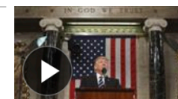
1. Oil Tankers Attacked in Gulf of Oman



2. Huawei's Chinese Phones Are Also American



3. Here's Where Some Lawmakers Hope to Reduce Trump's Power



4. Hong Kong Police Fire Tear Gas at Protesters



5. Why the CIA Cultivated Kim Jong Un's Half Brother as a Source



Most Popular Articles

1. Opinion: Netflix's False Story of the Central Park Five



2. Tankers Off Iran Hit by Suspected Torpedoes

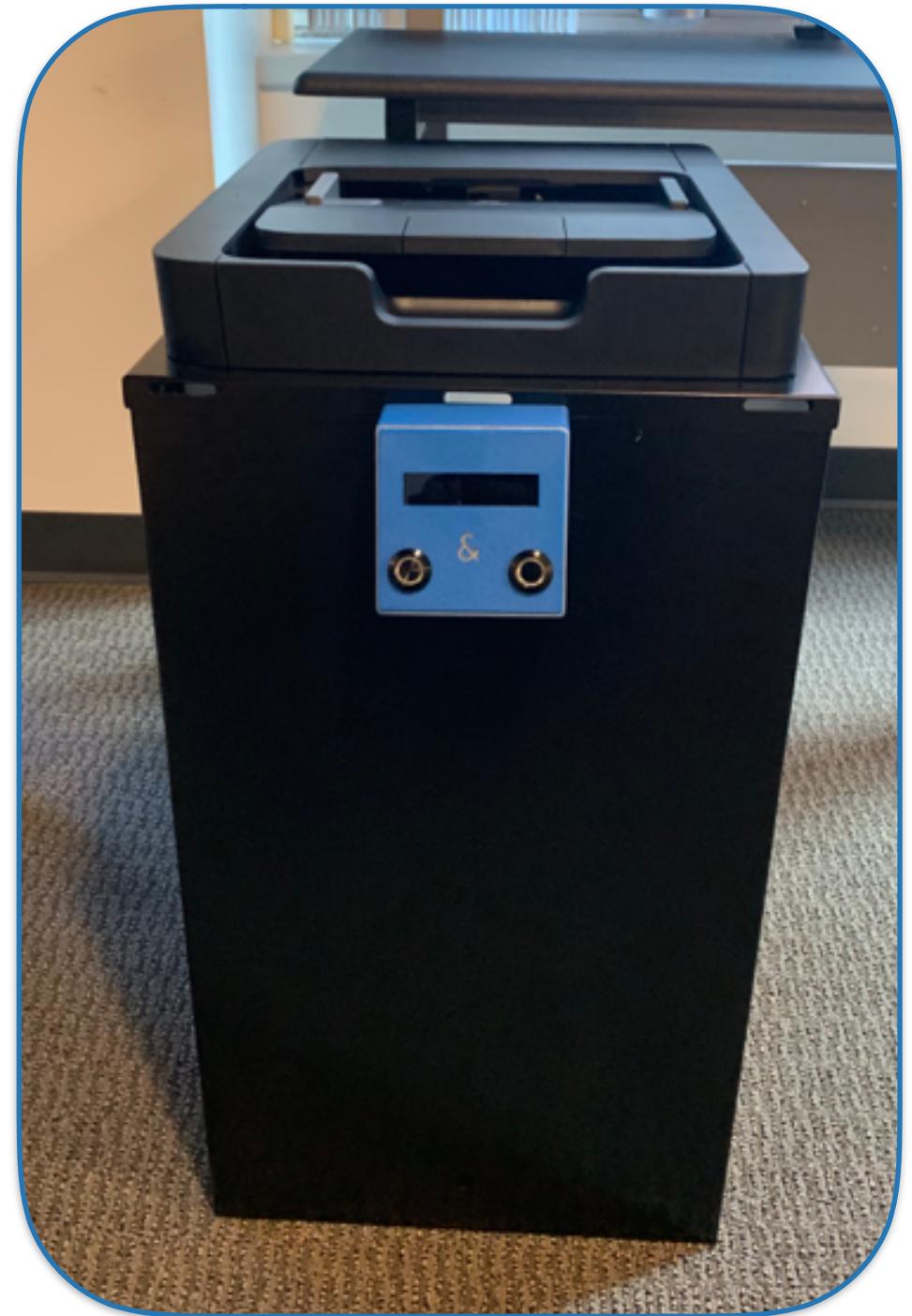


3. Facebook Emails Suggest Zuckerberg Knew of Problematic Privacy Practices

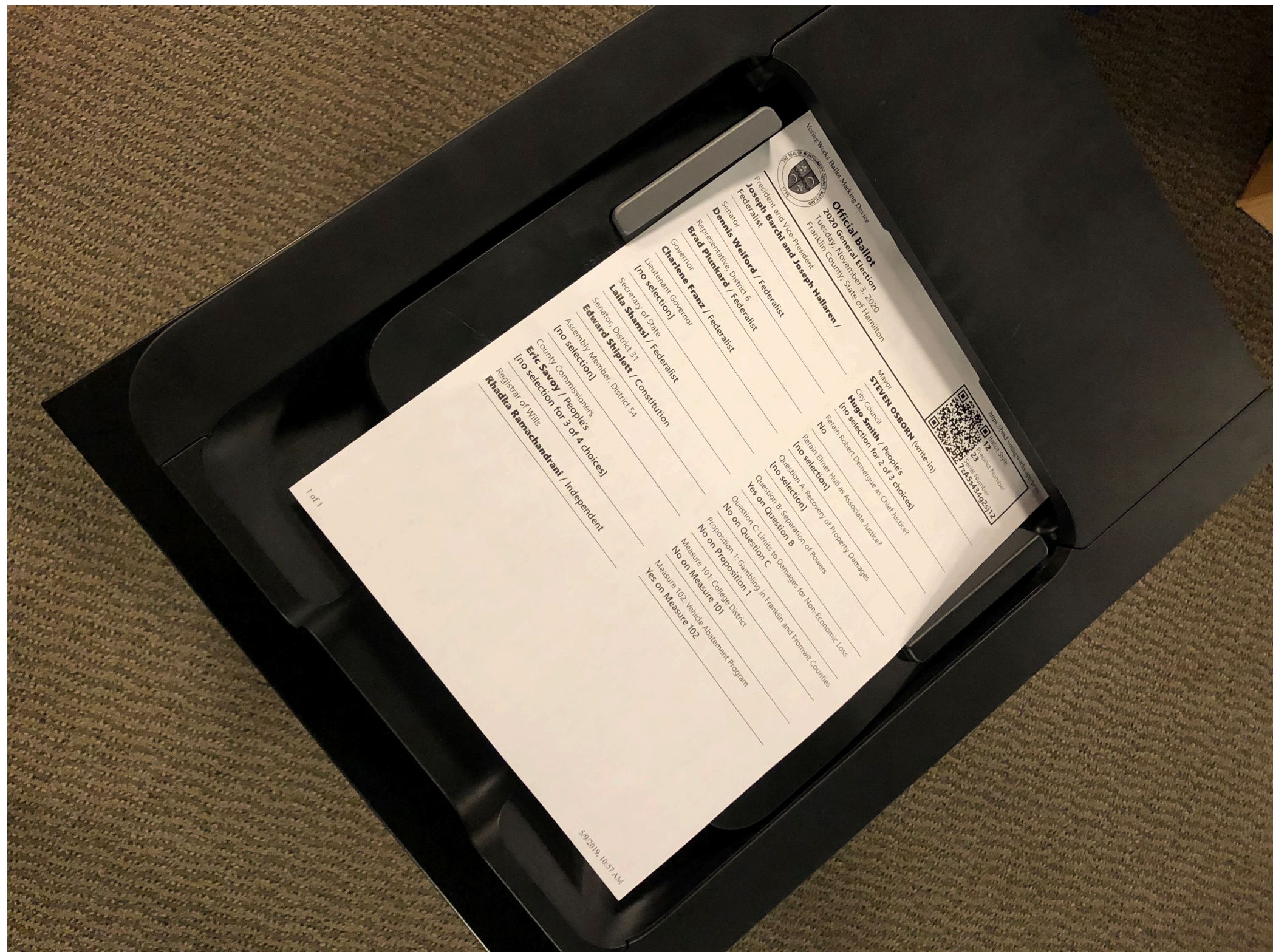


DARPA Secure Hardware meets Democracy

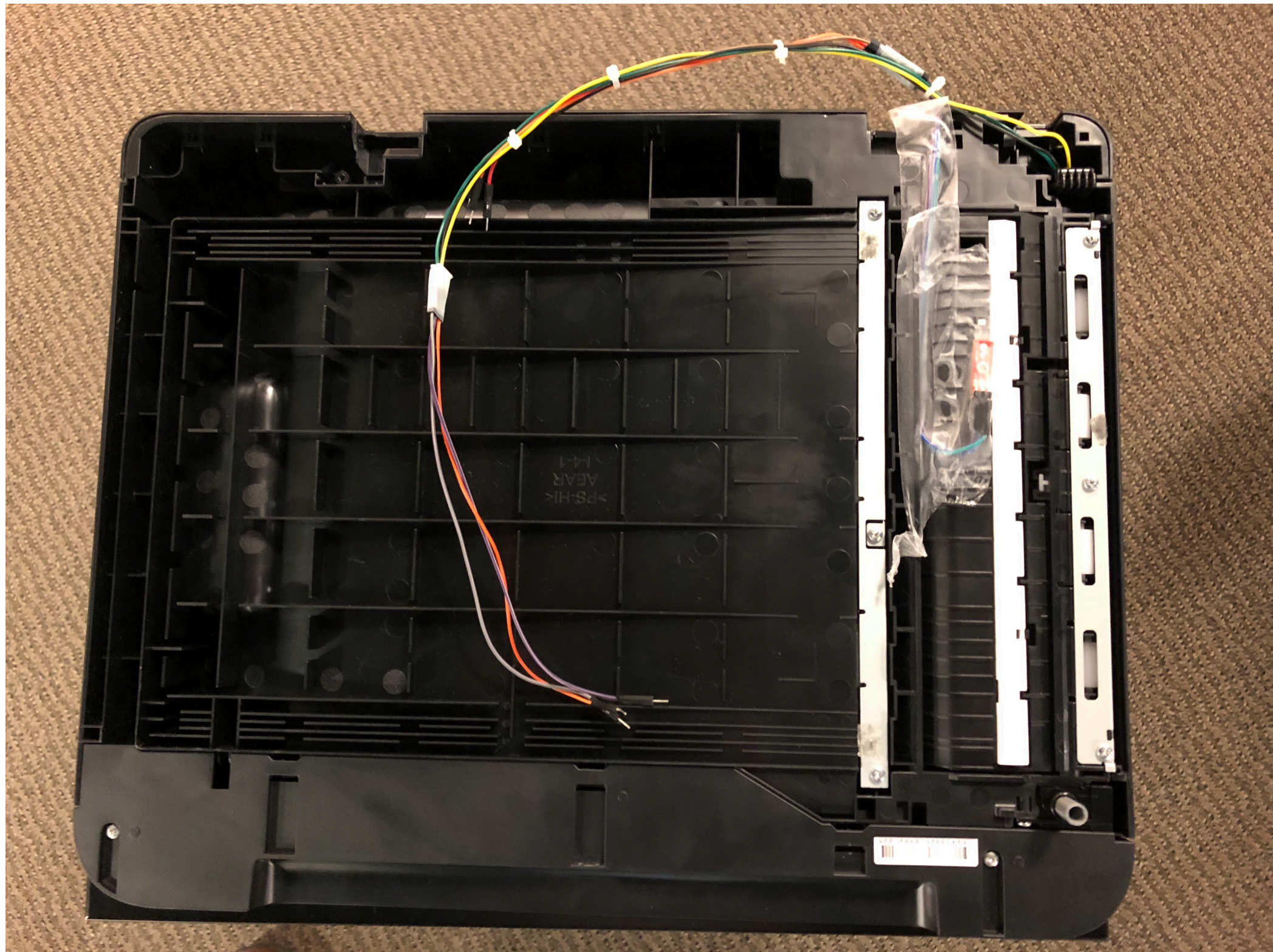
- election technology...
- is on everyone's minds
- is nationally critical infrastructure
- is notorious for security flaws
- a modern voting system...
- needs a microcontroller (in the ballot box that accepts paper ballots),
- a desktop CPU (for pollbooks, ballot marking devices, and hand-marked paper ballot scanning), and
- a superscalar CPU (for tabulation and reporting evidence to the public)
- must be open hardware and software



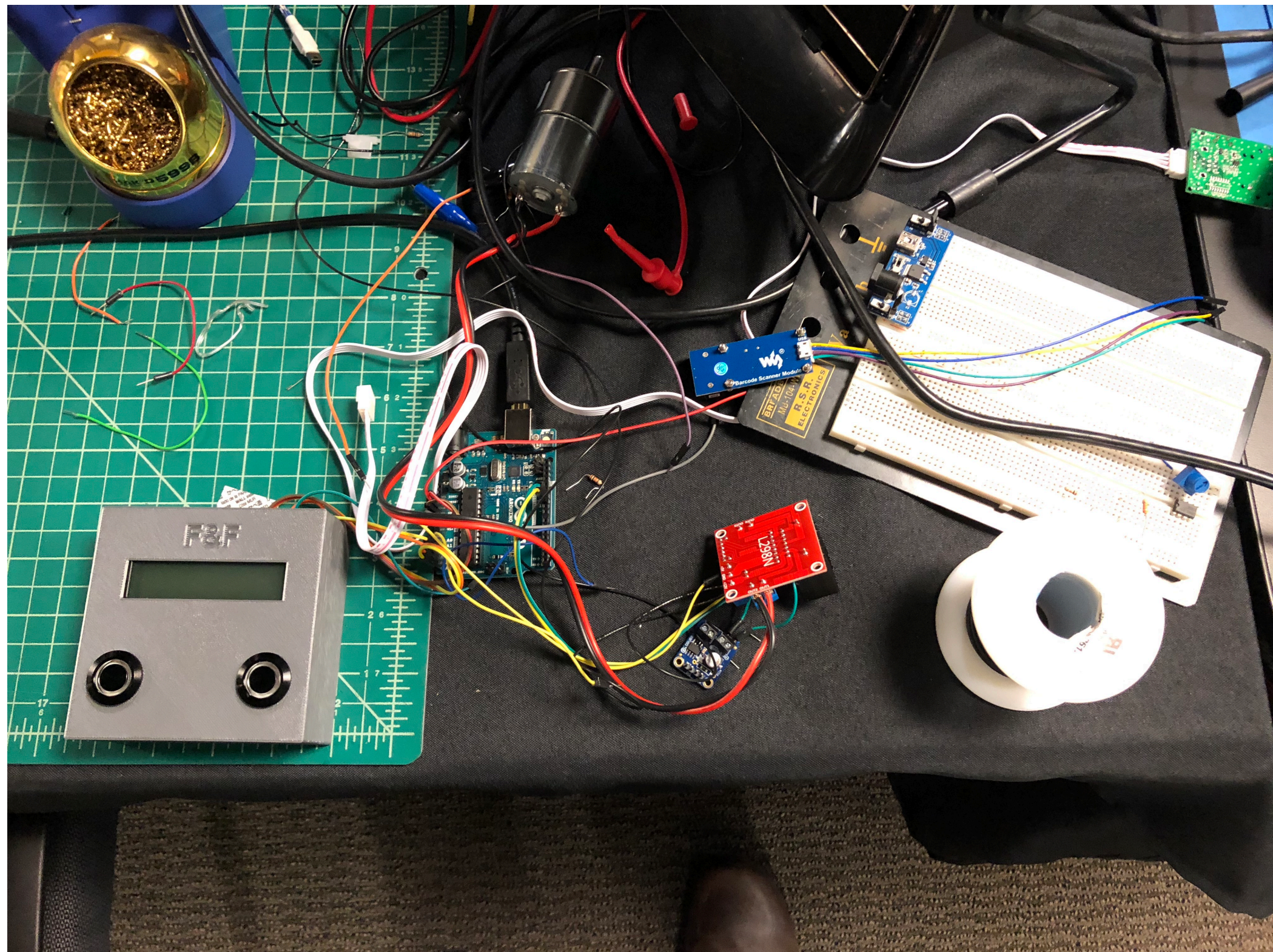
DEF CON 2019 Smart Ballot Box



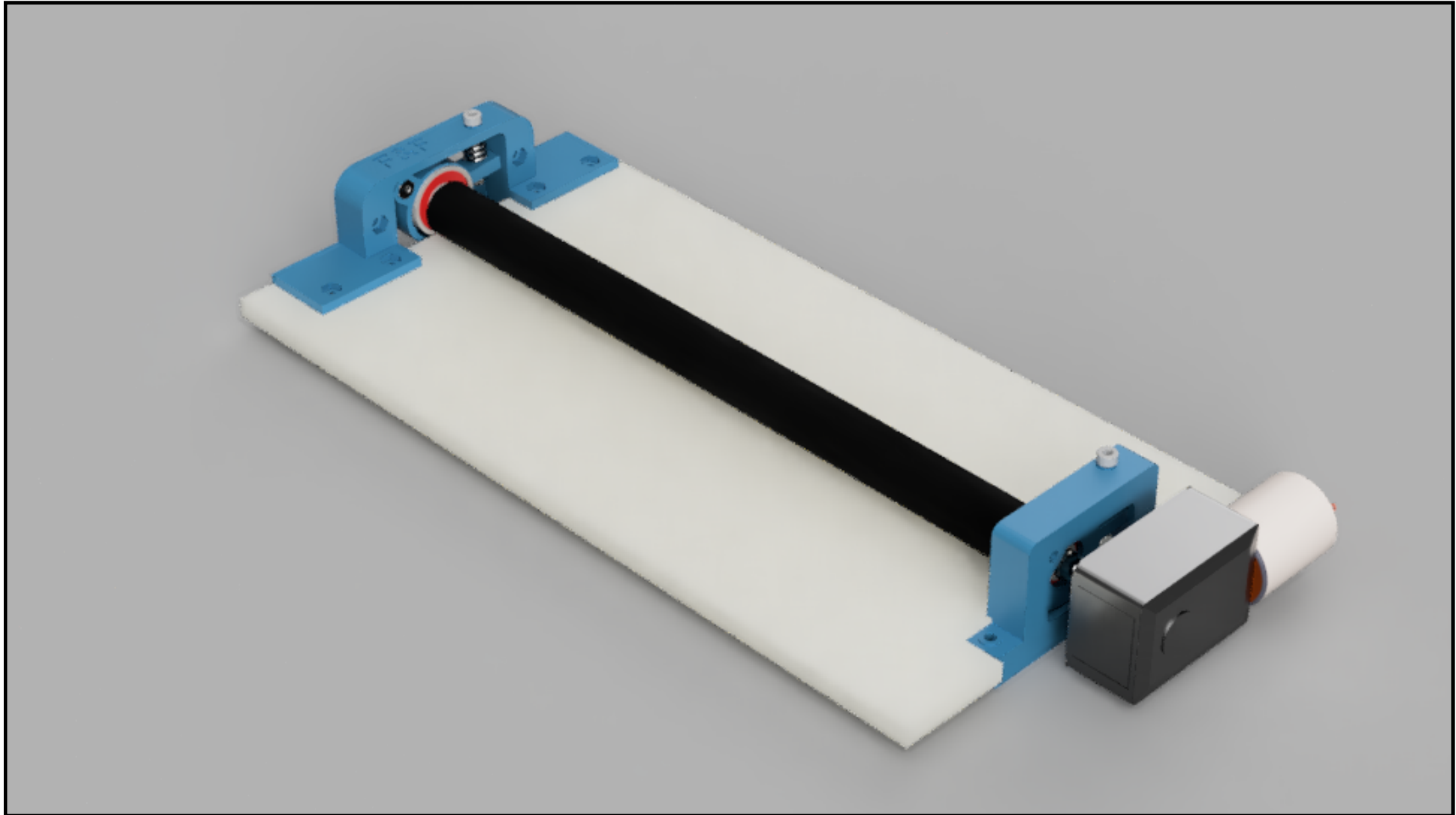
Smart Ballot Box (Reverse)



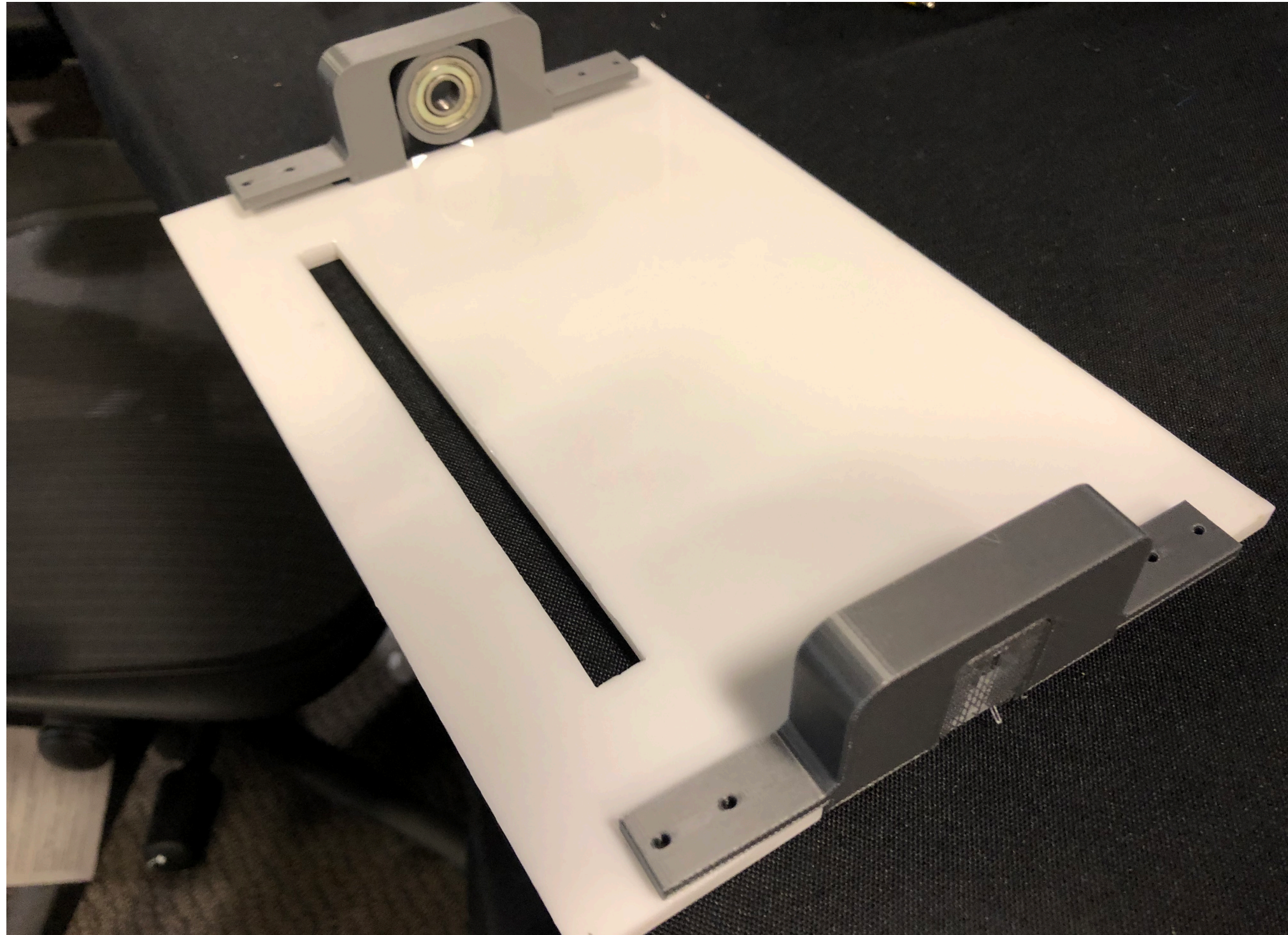
Smart Ballot Box Prototype



CAD SBB Mechanical Design



Physical Prototypes



DEF CON DARPA

Public Demonstration of Secure Hardware

- publish all source code, all firmware, and all hardware designs down to the RTL
- publish all hardware designs (CAD, PCBs, etc.)
- publish all documents describing the system: peer-reviewed papers, technical reports, threat models, assumptions and assurance case, etc.
- 2019: permit red team members to digitally attack external interfaces (serial and Ethernet) and load arbitrary malware into FreeRTOS on microcontroller
- 2020: same adversarial capability but targeting Linux and FreeBSD on two 64 bit SoCs

For More Information



- Galois <https://galois.com/>
- Free & Fair <https://freeandfair.us/>
- RISC-V <https://riscv.org/>
- <https://twitter.com/galois> @galois
- https://twitter.com/free_and_fair @free_and_fair
- <https://twitter.com/votingvillagedc> @votingvillagedc